© Prokurator Generalny – Minister Sprawiedliwości

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

Warszawa 2017

CZWARTA SEKCJA

**SPRAWA SZABÓ I VISSY PRZECIWKO WĘGROM**

*(Skarga nr 37138/14)*

WYROK

STRASBURG

12 stycznia 2016

OSTATECZNY

06/06/2016

*Wyrok ten stał się ostateczny zgodnie z art. 44 ust. 2 Konwencji. Może podlegać korekcie wydawniczej.*

W sprawie Szabó i Vissy przeciwko Węgrom,

Europejski Trybunał Praw Człowieka, zasiadając, jako Izba w składzie:

 Vincent A. De Gaetano, *Przewodniczący,* András Sajó, Boštjan M. Zupančič, Nona Tsotsoria, Paulo Pinto de Albuquerque, Krzysztof Wojtyczek, Iulia Antoanella Motoc, *sędziowie,*
oraz Fatoş Aracı, *zastępca Kanclerza Sekcji,*

Obradując na posiedzeniu niejawnym w dniach 14 kwietnia i 15 grudnia 2015 r.,

Wydaje następujący wyrok, który został przyjęty w ostatnim wspomnianym dniu:

POSTĘPOWANIE

1.  Sprawa wywodzi się ze skargi wniesionej do Trybunału (nr 37138/14) przeciwko Węgrom na podstawie art. 34 Konwencji o ochronie praw człowieka i podstawowych wolności („Konwencja”) przez dwóch obywateli węgierskich, Pana Máté Szabó i Pani Beatrix Vissy („skarżących”) w dniu 13 maja 2014 r.

2.  Skarżący byli reprezentowani przez Pana L. Majtényi, prawnika praktykującego w Budapeszcie, zaś Rząd węgierski („Rząd”) przez Pana Z. Tallódi, swego pełnomocnika z Ministerstwa Sprawiedliwości.

3.  Skarżący na podstawie art. 8. zarzucali, że mogli zostać potencjalnie poddani nieuzasadnionym i nieproporcjonalnym inwazyjnymi środkom w ramach „nadzoru określonego w art. 7/E (3)” (zobacz paragrafy 10—12 poniżej), w szczególności z powodu braku kontroli sądowej. W ich opinii ta ostatnia kwestia stanowiła również naruszenie praw wynikających z art. 6 i 13 Konwencji.

4.  W dniu 12 czerwca 2014r. skarga została zakomunikowana Rządowi.

5.  Odpowiednio: w dniach 27 sierpnia i 1 września 2014r., dwóm organizacjom pozarządowym Privacy International oraz Center for Democracy and Technology zostało przyznane prawo do przedłożenia pisemnych uwag (artykuł 36 ust. 2 Konwencji oraz Reguła 44 § 3 Regulaminu Trybunału).

FAKTY

I.  OKOLICZNOŚCI SPRAWY

6.  Skarżący urodzili się, odpowiednio, w 1976 r. i 1986 r. i mieszkają w Budapeszcie.

7.  W momencie wnoszenia skargi, skarżący byli członkami *Eötvös Károly Közpolitikai Intézet*, pozarządowej organizacji, “obserwatora” krytykującego Rząd. Następny pracodawca jednego ze skarżących był poddany kontroli finansowej wszczętej przez Rząd w 2014 r., która zdaniem skarżących była bliska dręczeniu.

8.  Ustawa nr CXLVII z 2010r. stanowi, że zwalczanie terroryzmu jest jednym z zadań Policji. Na jej mocy, w dniu 1 stycznia 2011 r. została powołana specjalna grupa zadaniowa ds. zwalczania terroryzmu („TEK”). Kompetencje tej grupy zostały zdefiniowane w artykule 7/E Ustawy nr XXXIV z 1994 o Policji, znowelizowanej ustawą nr CCVII z 2011r. („Ustawa o Policji”).

9.  W ramach tego ustawodawstwa, prerogatywy TEK w zakresie tajnego gromadzenia informacji wywiadowczych obejmują tajne przeszukiwanie domu oraz inwigilacja wraz z nagrywaniem, otwieranie listów i paczek, jak również sprawdzanie i nagrywanie treści elektronicznej lub skomputeryzowanej komunikacji bez zgody zainteresowanej osoby.

10.  Proces autoryzacji tych czynności jest uzależniony od rzeczywistych kompetencji wykonywanych przez TEK, a mianowicie tego czy mieszczą się one w ramach tajnej inwigilacji związanej z prowadzeniem dochodzenia w sprawie przestępstw enumeratywnie wymienionych w przepisach prawa (artykuł 7/E (2)) lub inwigilacji w ramach gromadzenia danych wywiadowczych dla bezpieczeństwa narodowego (artykuł 7/E (3)).

11.  Podczas gdy scenariusz z artykułu 7/E (2) podlega jako taki sądowej autoryzacji, to ten z artykułu 7/E (3) podlega autoryzacji przez Ministra Sprawiedliwości, (i) w celu zapobiegania atakom terrorystycznym lub w celu ochrony interesu bezpieczeństwa Węgier albo (ii) w celu ochrony obywateli przed schwytaniem za granicą w strefach wojny lub w związku z atakami terrorystycznymi.

12.  „Artykuł 7/E (3) inwigilacja” jest stosowany zgodnie z zasadami wynikającymi z ustawy o bezpieczeństwie narodowym, pod warunkiem, że nie można uzyskać niezbędnej informacji wywiadowczej w żaden inny sposób. W innym przypadku ustawa nie zawiera żadnych szczególnych przepisów dotyczących okoliczności, w których środek ten może zostać zarządzony, w przeciwieństwie do „artykułu 7/E (2) inwigilacja”, którego zastosowanie jest uzależnione od podejrzenia popełnienia pewnych poważnych przestępstw. Ramy czasowe inwigilacji określonej w artykule 7/E (3)” wynoszą 90 dni, co może zostać przedłużone przez Ministra o kolejne 90 dni, jakkolwiek nie może on znać wyników kontroli operacyjnej w momencie podejmowania decyzji o przedłużeniu. Po zakończeniu trwania wspomnianego środka, prawo nie nakłada na władze żadnego szczególnego obowiązku niszczenia wszelkich pozyskanych danych wywiadowczych, które okazały się nieistotne.

13.  W dniu 15 czerwca 2012 r. skarżący wnieśli skargę konstytucyjną, argumentując zasadniczo, że prerogatywy przewidziane w artykule 7/E (3) naruszyły ich konstytucyjne prawo do prywatności. Podkreślili oni, że ustawodawstwo dotyczące środków inwigilacji do celów bezpieczeństwa narodowego zapewnia mniej gwarancji ochrony prawa do prywatności niż przepisy dotyczące inwigilacji związanej z prowadzeniem dochodzenia w sprawie poszczególnych przestępstw. Wskazali oni, że (i) „inwigilacja określona w art. 7/E ust. 2” jest zawsze związana z konkretnym przestępstwem i może zostać zarządzona jedynie w celu identyfikacji lub zlokalizowania podejrzanych, podczas gdy stosowanie tej z artykułu 7/E (3) nie jest związane z żadnym konkretnym przestępstwem; (ii) „artykuł 7/E (2) inwigilacja” jest stosowany przez sąd, podczas gdy „artykuł 7/E (3) inwigilacja” podlega zatwierdzeniu przez ministra właściwego do spraw sprawiedliwości; (iii) sądowe zastosowanie „artykułu  7/E (2) inwigilacja” podlega szczegółowemu uzasadnieniu, a wydanie decyzji przez ministra na podstawie „artykułu 7/E (3) inwigilacja” nie wymaga wydania uzasadnienia; oraz (iv) na mocy przepisów odnoszących się do „artykułu 7/E (2) inwigilacja” wszystkie zebrane, ale nieistotne informacje musiały zostać zniszczone w przeciągu ośmiu dni, kwestia ta wygląda zgoła inaczej w „artykule 7/E (3) inwigilacja”.

14.  W dniu 18 listopada 2013 r. Trybunał Konstytucyjny oddalił większość zarzutów skarżących. Niemniej zgodził się ze skarżącymi w jednym aspekcie, a mianowicie stwierdził, że decyzja ministra zezwalająca na gromadzenie informacji wywiadowczych musi podlegać uzasadnieniu. Pomimo tego, Trybunał Konstytucyjny zasadniczo orzekł, że zakres zadań związanych z bezpieczeństwem narodowym był znacznie szerszy niż zakres zadań związanych z prowadzeniem dochodzenia w sprawie pewnych przestępstw. Dla celów bezpieczeństwa narodowego wydarzenia z rzeczywistości nie były badane pod kątem ich znaczenia z punktu widzenia prawa karnego, dlatego też nie muszą one koniecznie być związane z konkretnym przestępstwem.Ponadto w kontekście bezpieczeństwa narodowego, zewnętrzna kontrola jakiejkolwiek inwigilacji, na którą zgodę wyraził minister, sprawowana była przez parlamentarną komisję bezpieczeństwa narodowego (która miało prawo do wezwania ministra w celu złożenia wyjaśnień, zarówno w kwestiach ogólnych, jaki i w konkretnych sprawach) oraz Rzecznika Praw Obywatelskich, system ten był wystarczający do zagwarantowania poszanowania konstytucyjnego prawa do prywatności zainteresowanym stronom. Trybunał Konstytucyjny ostatecznie był zdania, że Ustawa o bezpieczeństwie narodowym, stosownie do „artykułu 7/E (3) inwigilacji”, zawierała ogólne przepisy o usunięciu z urzędu wszelkich niepotrzebnych danych do osiągnięcia celu leżącego u podstaw gromadzenia danych wywiadowczych.

15.  Orzeczenie to zostało opublikowane w Dzienniku Urzędowym z dnia 22 listopada 2013 r.

II.  WŁAŚCIWE PRAWO KRAJOWE

16.  Ustawa nr XXXIV z 1994 o Policji („Ustawa o Policji”) stanowi odpowiednio:

Artykuł 1

„(2) Policja – w ramach swoich obowiązków określonych w Ustawie Zasadniczej Węgier, w niniejszej ustawie oraz w innych ustawach o zapobieganiu i zwalczaniu przestępstw, administrowaniu i nadzorowaniu porządku publicznego–...

15. ... na obszarze Węgier ...

a) śledzi organizacje terrorystyczne,

b) zapobiega, śledzi i odpiera wszelkie próby przeprowadzenia ataku terrorystycznego przez jednostki, grupy lub organizacje oraz utrudnia popełnianie przez nich przestępstw,

c) utrudnia jednostkom, grupom lub organizacjom finansowe lub inne wspieranie operacji organizacji terrorystycznych.”

Artykuł 7/E

„(1) Organ antyterrorystyczny nie posiada kompetencji dochodzeniowych. Organ ten:

a) wypełnia zadania określone w art. 1 ust. 2 pkt. 15, a w ramach tych zadań ...

ad) – w ramach walki z terroryzmem oraz w celu ochrony interesu bezpieczeństwa Węgier – zapobiega, śledzi i odpiera wszelkie próby przeprowadzenia ataku terrorystycznego (*terrorcselekmény*) na Węgrzech. ...

d) na podstawie decyzji Ministra właściwego do spraw porządku publicznego, wydanej za zgodą Ministra właściwego do spraw zagranicznych – w zgodzie z zasadami prawa międzynarodowego - bierze udział w ratowaniu obywateli Węgier, którzy są – poza terytorium Węgier – w niebezpieczeństwie bezpośredniego zagrożenia życia spowodowanego groźbą wybuchu wojny, zbrojnym konfliktem, pojmaniem, jako zakładnicy lub działaniem terrorystycznym; w celu zapewnienia im bezpiecznego powrotu na Węgry oraz przeprowadzenia ewakuacji; w tym celu współpracuje z Państwami Członkowskimi Unii Europejskiej oraz jej organami, z organami Organizacji Traktatu Północnoatlantyckiego, z powiązanymi organizacjami międzynarodowymi i władzami zainteresowanego obcego państwa.

e) pozyskuje, analizuje, ocenia i przekazuje informacje odnoszące się do państw obcych lub informacje będące obcego pochodzenia, które są niezbędne do realizacji zadań określonych w punkcie d) powyżej.

(2) Organ antyterrorystyczny może- dla celów związanych z wypełnieniem swoich zadań z ustępu (1) punktu a) podpunktu aa) do ac) oraz z punktu c) – gromadzić informacje wywiadowcze zgodnie z przepisami rozdziału VII Ustawy o Policji.

(3) Organ antyterrorystyczny może – dla celów związanych z wypełnieniem swoich zadań z ustępu 1) punktu a) podpunktu ad) oraz z punktu e) – gromadzić informacje wywiadowcze zgodnie z przepisami artykułów 53-60 Ustawy nr CXXV z 1995 r. o Narodowych Służbach Bezpieczeństwa („Nbtv.”), podczas których może żądać i przetwarzać dane zgodne z przepisami artykułów 38-52 Nbtv. Gromadzenie informacji wywiadowczych zostało przewidziane w artykule 56 punktach a)-e) Nbtv., wymaga zezwolenia Ministra właściwego do spraw sprawiedliwości.”

Przestępstwo „ataku terrorystycznego” (*terrorcselekmény*) zostało zdefiniowane w art. 261 starego Kodeksu karnego oraz w art. 314 – 316 nowego Kodeksu karnego.

17.  Ustawa nr CXXV z 1995r. o Narodowych Służbach Bezpieczeństwa („o Bezpieczeństwie Narodowym”, „Nbtv.”) przewiduje jak w poniższych fragmentach.

Zgodnie z artykułem 11(5), skargi na czynności organu antyterrorystycznego są rozpatrywane przez Ministra Spraw Wewnętrznych, który w terminie 30 dniu zawiadamia skarżących o wyniku przeprowadzonego przez siebie postępowania oraz o podjętych w tym przedmiocie środkach (termin ten może, w konkretnych przypadkach zostać przedłużony o kolejne 30 dni).

Artykuł 14(4) zawiera postanowienia dotyczące istotnych kompetencji Komisji Bezpieczeństwa Narodowego. Sprawując nadzór parlamentarny, Komisja ma prawo wezwać Ministra oraz dyrektorów krajowych służb bezpieczeństwa do udzielenia informacji w zakresie bezpieczeństwa narodowego oraz funkcjonowania i działalności służb (ustęp (a)).

W postępowaniach ze skarg indywidualnych, kiedy skarżący nie zgadza się z wynikiem dochodzenia prowadzonego zgodnie z artykułem 11(5), Komisja może przeprowadzić dochodzenie z tytułu rzekomo bezprawnego działania Narodowych Służb Bezpieczeństwa, jeżeli powaga sprawy to uzasadnia, a za przyjęciem skargi musi głosować, co najmniej jedna trzecia członków Komisji. Prowadząc dochodzenie Komisja bada skargę i może zwrócić się do Ministra o wydanie opinii w tej sprawie. Jeżeli Komisja jest zdania, że działanie służb było niezgodne z prawem lub stanowiło nadużycie, może zwrócić się do Ministra o przeprowadzenie dochodzenia i o informowanie Komisji o wynikach dochodzenia albo też Komisja może sama przeprowadzić dochodzenie wyjaśniające, jeżeli ma wrażanie, że działania służb są w sprzeczności z odpowiednimi przepisami prawa. Prowadząc dochodzenie wyjaśniające Komisja może dokonać sprawdzenia istotnych dokumentów znajdujących się w rejestrze Narodowych Służb Bezpieczeństwa oraz może przesłuchać personel Narodowych Służb Bezpieczeństwa. Opierając się na swoich ustaleniach Komisja może zwrócić się do Ministra o podjęcie niezbędnych działań.

Artykuł 43

“Narodowe Służby Bezpieczeństwa mogą wykorzystywać informacje, o których się dowiedziały, wyłącznie do celów, które są w zgodzie z tymi, które leżą u podstaw do ich pozyskania, z wyjątkiem:

a) informacji, które wskazują, że doszło do popełnienia czynu zabronionego, a przekazywanie ich jest zgodne z prawem, albo

b) jeżeli uzasadniają one obowiązek poinformowania innych Narodowych Służb Bezpieczeństwa, a podmiot ten jest sam upoważniony do ich otrzymywania.”

Artykuł 44

„(1) Narodowe Służby Bezpieczeństwa, do celów związanych z wypełnianiem swoich zadań mogą od siebie nawzajem żądać informacji oraz są zobowiązane do przekazywania tych informacji sobie nawzajem, zgodnie z postanowieniami niniejszej ustawy.

(4) Organy wnoszące o ujawnienie informacji są odpowiedzialne za zarządzanie informacjami im ujawnionymi, zgodnie z przepisami niniejszej ustawy oraz ustawodawstwem odnoszącym się do zarządzania informacjami; rejestrują informacje, które otrzymały oraz ich wykorzystywanie, a także, na wniosek, informują o tym Narodowe Służb Bezpieczeństwa.”

Artykuł 45

„(1) Narodowe Służby Bezpieczeństwa mogą, na mocy zobowiązania międzynarodowego, przekazać dane osobowe zagranicznym organom przetwarzania danych w ramach przepisów dotyczących ochrony danych osobowych,.”

Artykuł 50

„(2) Dane osobowe przetwarzane przez Narodowe Służby Bezpieczeństwa zostaną natychmiast usunięte, jeżeli

a) okres ustalony w ustępie (1) minął;

b) o usunięciu orzekł sąd w postępowaniu dotyczącym ochrony danych;

c) przetwarzanie danych jest niezgodne z prawem;

d) zostały spełnione warunki z artykułu 60 (2);

e) przetwarzanie danych stało się oczywiście niepotrzebne.”

Artykuł 53

„(2) Narodowe Służby Bezpieczeństwa mogą zastosować specjalne środki i metody gromadzenia tajnych danych wywiadowczych tylko, jeżeli dane wywiadowcze konieczne do wypełnienia obowiązków wynikających z niniejszej ustawy nie mogą zostać uzyskane w żaden inny sposób.”

Artykuł 56

“Narodowe Służby Bezpieczeństwa mogą na podstawie zewnętrznego pozwolenia

a) tajnie przeszukiwać pomieszczenia i nagrywać za pomocą sprzętu technicznego, to, co zostanie zaobserwowane;

b) utrzymywać pomieszczenie pod obserwacją i nagrywać za pomocą sprzętu technicznego to, co zostanie zaobserwowane;

c) otwierać i sprawdzać pocztę oraz wszystkie zamknięte paczki należące do nieokreślonej osoby oraz nagrywać, za pomocą sprzętu technicznego tego, co jest w nich zawarte;

d) wykrywać treść komunikatów przekazywanych droga elektroniczną oraz nagrywać to za pomocą sprzętu technicznego;

e) wykrywać dane przekazywane lub zawarte w komputerze lub sieci, nagrywać je za pomocą sprzętu technicznego oraz wykorzystywać je.”

Artykuł 57

„(1) Wniosek o udzielenie zezwolenia na gromadzenie tajnych danych wywiadowczych, tak jak zostało sprecyzowane w artykule 56, może zostać złożony przez dyrektorów generalnych Organów Informacyjnych, urząd Ochrony Konstytucji, Wojskową Służbę Bezpieczeństwa Narodowego oraz – w celu w realizacji swoich zadań określonych w artykule 8 (1) f) powyżej – Specjalną Służbę Bezpieczeństwa Narodowego.

(2) Wniosek powinien zawierać:

a) teren gromadzenia tajnych danych wywiadowczych, zainteresowaną osobę (osoby), określoną z imienia i nazwiska lub jako grupa osób i/albo wszelkie inne informacje umożliwiające identyfikację takiej osoby lub osób;

b) wskazanie gromadzonych danych wywiadowczych oraz uzasadnienie potwierdzające taką konieczność;

c) datę rozpoczęcia i zakończenia tego działania;

d) w przypadku wniosku o uzyskanie zezwolenia określonego w artykule 59 poniżej, uzasadnienie, dlaczego gromadzenie danych wywiadowczych jest absolutnie konieczne w określonych okolicznościach sprawy do sprawnego funkcjonowanie Służby Bezpieczeństwa Narodowego.”

Artykuł 58

“(3) ... Minister właściwy do spraw wymiaru sprawiedliwości ... decyduje [w sprawie wniosku] w ciągu 72 godzin liczonych od złożenia wniosku o udzieleniu zezwolenia lub, gdy żądanie jest nieuzasadnione o jego odrzuceniu. Decyzja ta jest niezaskarżalna.

(4) O ile przepisy prawa nie stanowią inaczej, zezwolenia na gromadzenie tajnych danych wywiadowczych udziela się na maksymalny okres 90 dni na każdy wniosek. W uzasadnionych wypadkach oraz jeżeli wniosek został złożony przez dyrektora generalnego, okres ten może zostać przedłużony o 90 dni, chyba że przepisy prawa stanowią inaczej.

(6) Osoba w stosunku do której prowadzone jest postępowanie nie jest o nim informowana, nie jest też informowana o gromadzeniu o niej danych wywiadowczych..”

Artykuł 59

“(1) Dyrektorzy Służb Bezpieczeństwa Narodowego mogą [wyjątkowo] udzielić zezwolenia na gromadzenie danych wywiadowczych w rozumieniu artykułu 56 -najpóźniej do czasu wydania decyzji [przez Ministra], jeżeli zewnętrza procedura udzielania zezwoleń pociąga za sobą takie opóźnienie, że w danych okolicznościach w sposób oczywisty jest to sprzeczne z interesem skutecznego funkcjonowania Służby Bezpieczeństwa Narodowego.”

Artykuł 60

„(1) Niezwłocznie zaniecha się gromadzenia danych wywiadowczych, opartego na zewnętrznej decyzji, jeżeli

a) cel określony w zezwoleniu został osiągnięty;

b) kontynuacja gromadzenia nie przyniesie żadnych efektów;

c) czas minął i nie był przedłużany;

d) gromadzenie danych wywiadowczych jest z jakiegokolwiek powodu bezprawne.

(2) W ramach specjalnej procedury określonej w artykule 59 (1), zaniecha się niezwłocznie gromadzenia danych wywiadowczych, jeżeli nie zostanie wydane pozwolenie na jego kontynuację. W tym wypadku informacje zgromadzone zostaną niezwłocznie usunięte, zgodnie z przepisami prawa o usuwaniu danych kwalifikowanych.”

W artykule 74(a) pojęcie zabezpieczenia interesu narodowego zostało zdefiniowane w następujący sposób:

„Zabezpieczenie suwerenności oraz ochrona porządku konstytucyjnego na Węgrzech, w tym

aa) pozyskiwanie informacji wywiadowczych dotyczących agresywnych działań wymierzonych w niepodległość i jedność terytorialną kraju,

ab) pozyskiwanie informacji wywiadowczych oraz zwalczanie działań naruszających lub zagrażających interesowi politycznemu, ekonomicznemu lub obronnemu kraju,

ac) pozyskiwanie informacji o zagranicznym znaczeniu lub pochodzeniu, które są wymagane przy podejmowaniu rządowych decyzji,

ad) pozyskiwanie informacji wywiadowczych oraz zwalczanie działań zmierzających w sposób bezprawny do zmiany lub zakłócenia państwowego porządku konstytucyjnego, gwarantującego przestrzeganie fundamentalnych praw człowieka, pluralistycznej demokracji przedstawicielskiej, organów konstytucyjnych oraz

ae) pozyskiwanie informacji wywiadowczych dotyczących zwalczania aktów terroryzmu, nielegalnego handlu bronią i narkotykami oraz nielegalny handel produktami i technologiami na poziomie międzynarodowym,”

18.  Ustawa nr CXI z 2011 r. o Komisarzu ds. Praw Podstawowych (“Ajbt.”), przewiduje że:

W artykule 18 (1) f), organy egzekwujące prawo – włączając w to organ antyterrorystyczny – podlegają postępowaniu prowadzonemu przez Rzecznika Praw Obywatelskich. Postępowanie rzecznika jest ograniczone tylko w jeden sposób: sprawozdanie dotyczące działań organów wywiadowczych uprawnionych do używania urządzeń wywiadowczych, nie może zawierać informacji, z których można wyciągnąć wniosek, że w danej sprawie działania wywiadowcze zostały przeprowadzone przez organ czy też nie [cf. artykuł 28(3)]. Komisarz ds. Praw Podstawowych corocznie składa sprawozdanie przed Parlamentem, dotyczące spraw, odnośnie do których prowadził postępowanie oraz może – za wyjątkiem propozycji wprowadzenia zmian – zażądać od Parlamentu zbadania każdej sprawy. Tam gdzie zostało stwierdzone nadużycie poufnych danych lub niewłaściwe administrowanie danymi, Komisarz ds. Praw Podstawowych jednocześnie z corocznym sprawozdaniem, jeżeli nadużycie poufnych danych lub niewłaściwe administrowanie danymi jest bardzo poważne lub dotyka znacznej liczby osób fizycznych, przed złożeniem corocznego sprawozdania- przekazuje w sprawozdaniu sprawę do odpowiedniej komisji parlamentarnej, sklasyfikowanym zgodnie z ustawą o ochronie danych poufnych.

Skarżący przedłożył zaświadczenie uzyskane z biura Komisarza z dnia 9 lipca 2014 r., zgodnie, z którym Komisarz nigdy nie pytał o kwestie dotyczące środków gromadzenia danych wywiadowczych.

19.  Ustawa nr CLI z 2011 roku o Trybunale Konstytucyjnym, stanowi następująco:

Artykuł 26 (1)

“Osoby lub organizacje dotknięte daną sprawą, zgodnie z artykułem 24 (2) c) Ustawy Zasadniczej mogą wnieść skargę konstytucyjną do Trybunału Konstytucyjnego, jeżeli z powodu zastosowania w postępowaniach sądowych aktu prawnego sprzecznego z Ustawą Zasadniczą,

a) ich prawa zawarte w Ustawie Zasadniczej został naruszone, oraz

b) środki prawne zostały wyczerpane, lub takowe środki nie istnieją.

(2) W drodze odstępstwa od ustępu 1, postępowanie przed Trybunałem Konstytucyjnym może również zostać zainicjowane, jeżeli

a) szkoda wynikła bezpośrednio z zastosowania lub wejścia w życie przepisu sprzecznego z Ustawą Zasadniczą, bez orzeczenia sądu, oraz

b) procedura odszkodowawcza za poniesioną szkodą nie jest dostępna lub gdy dostępne środki zostały już wykorzystane przez skarżącego. ...”

Artykuł 27

“Przeciwko orzeczeniu sądowemu, będącemu w sprzeczności z Ustawą Zasadniczą w rozumieniu artykułu 24 (2) d.) Ustawy Zasadniczej, osoba lub organizacja dotknięta daną sprawą może wnieść do Trybunału Konstytucyjnego skargę konstytucyjną, jeżeli rozstrzygnięcie co do istoty sprawy lub inna decyzja kończąca postępowanie sądowe

a) naruszyła prawa skarżącego zapisane w Ustawie Zasadniczej,

b) skarżący wykorzystał już istniejące środki prawne lub takowe nie istniały.”

20.  Decyzja nr 32/2013 (XI.22.) AB Trybunału Konstytucyjnego ustanawiająca wymóg konstytucyjny w odniesieniu do artykułu 58 (3) Nbtv. oraz odrzucająca podobną skargę konstytucyjną, zawiera następujące fragmenty:

“... 1. Trybunał Konstytucyjny stwierdza, że... aby zewnętrzna kontrola była efektywna, decyzja Ministra właściwego do spraw sprawiedliwości ... zatwierdzająca gromadzenie danych wywiadowczych musi zawierać uzasadnienie. ...

[42] 1.1. Obowiązujące regulacje wyróżniają dwa typy gromadzenia danych wywiadowczych: gromadzenie danych powiązanych z prowadzeniem dochodzeń w sprawie poszczególnych przestępstw oraz gromadzenie danych nie związanych z poszczególnymi przestępstwami. ...

[47] 1.2. Gromadzenie danych niepowiązanych z prowadzeniem dochodzenia w sprawie poszczególnych przestępstw albo nie jest przedmiotem zewnętrznej autoryzacji [artykuły 54-55 Nbtv.] albo jest przedmiotem takiej autoryzacji [artykuły 54-55 Nbtv.] W przypadkach określonych w Ustawie, autoryzacja oznacza autoryzację dokonaną przez sędziego lub Ministra sprawiedliwości.

[48] Zgodnie z uzasadnieniem do Nbtv., można wymienić kilka przykładów z praktyki międzynarodowej państw rozróżniających między gromadzeniem danych wywiadowczych związanych z prowadzeniem dochodzenia w sprawie poszczególnych przestępstw (w tym ściśle powiązanych dziedzin zapobiegania i wykrywania przestępczości oraz gromadzenia danych wywiadowczych dla celów bezpieczeństwa narodowego).

[49] Bazując na tej regule, do ustawy został wprowadzony podzielony system autoryzacji. W celu wykrywania rzeczywistych przestępstw, gromadzenie danych wywiadowczych jest autoryzowane – podobnie do rozwiązania zastosowanego w Ustawie o Policji- przez sędziego mianowanego do wykonywania tego zadania przez Prezesa Sądu Najwyższego w Budapeszcie, podczas gdy czynności przeprowadzone na podstawie artykułu 56 są autoryzowane przez Ministra Sprawiedliwości. ...

[51] Artykuł 53 (2) Nbtv., zgodnie z którym gromadzenie tajnych danych wywiadowczych może być przeprowadzone tylko, jeżeli dane potrzebne do wykonania ustawowych obowiązków nie mogą zostać uzyskane w inny sposób, znajduje zastosowanie do obu przypadków. ...

[62] Zgodnie z artykułem 14 (4) Nbtv. parlamentarna komisja ds. bezpieczeństwa narodowego sprawuje kontrolę nad procesem autoryzacji wykonywanym przez Ministra Sprawiedliwości. ...

[69] 2. Gromadzenie danych wywiadowczych na mocy Nbtv, niepowiązanych z prowadzeniem dochodzenia w sprawie poszczególnych przestępstw .... nie było do tej pory przedmiotem postępowania przed Trybunałem Konstytucyjnym. Jednakże, w swojej decyzji nr 2/2007. (I. 24.) AB (dalej: Abh.1.) Trybunał Konstytucyjny określił ogólne aspekty, zgodnie z którymi gromadzenie danych wywiadowczych jest dopuszczalne w demokratycznym państwie prawa.

[70] Z tego względu, że treść artykułu B) (1) Ustawy Zasadniczej jest identyczna z treścią artykułu 2 (1) poprzedniej Konstytucji, oraz że z zasad wykładni odnoszących się do Ustawy Zasadniczej nie można wywnioskować niczego sprzecznego z powyższą opinią Trybunał Konstytucyjnego, można podtrzymać twierdzenia co do zasady i co do konieczności i proporcjonalności gromadzenia informacji wywiadowczych.

[71] Trybunał Konstytucyjny wziął, również pod rozwagę orzecznictwo Strasburskiego Trybunału, które przywoływał w swoich poprzednich orzeczeniach. Sprawy związane z „ukrytym dochodzeniem” były przedmiotem badania Trybunału w świetle postanowień Konwencji określonych w artykule 8, który chroni prawo do poszanowania życia prywatnego. W swoich orzeczeniach Trybunał orzekał, że w społeczeństwie demokratycznym, prawa wyrażone w art. 8 ust. 1 mogą być ograniczone tylko w granicach przewidzianych przez ustęp 2, to jest, tylko dla celów określonych w tym przepisie i tylko, kiedy konieczność ograniczenia jest uzasadniona w sprawie.

[72] Legalność, zgodnie z orzecznictwem Trybunału nie tylko wymaga, żeby dane ograniczenie było przewidziane prawem. Termin „zgodnie z prawem” stanowi, że przepis sam w sobie musi być zgodny z zasadami państwa prawa. Z tego względu, że tajne gromadzenie danych wywiadowczych, samo przez się wyłącza możliwość skutecznego środka, koniecznym jest, aby proces zatwierdzenia gromadzenia takich informacji zawierał wystarczające gwarancje do ochrony praw podmiotów indywidualnych. Stąd też, korzystanie z gromadzenia danych wywiadowczych musi być przedmiotem trzy etapowej kontroli: kiedy ingerencja jest zarządzana, kiedy ingerencja jest przeprowadzana oraz kiedy ingerencja jest zakończona. Kontrola musi być przeprowadzona przez organy niezależne od władzy wykonawczej. Po pierwsze, tylko ciągła, trwająca i obligatoryjna kontrola może dawać gwarancję, że w danej sprawie wymóg proporcjonalności nie zostanie naruszony ...

[73] W swoim orzecznictwie Trybunał położył nacisk na minimalne wymagania, jakie musi spełniać regulacja prawna w przedmiocie korzystania z urządzeń danych wywiadowczych. Trybunał podkreślał, że ponieważ ingerencja w podstawowe prawa jest tajna oraz że użycie takich mechanizmów daje władzy wykonawczej „nieprzewidywalne” możliwości, niezbędnym jest, żeby procedury same w sobie zapewniały wystarczające gwarancje przestrzegania praw jednostek. W związku z tym Państwa muszą stworzyć precyzyjne i szczegółowe zasady, które muszą być przestrzegane i dostępne dla obywateli. Kompetencje organu stosującego takie urządzenia, istota środków oraz sposób ich stosowania powinien jasno i oczywiście wynikać z regulacji prawnych. Co do wymagania jasności zasad, Trybunał wskazał również, że prawo powinno definiować wypadki i okoliczności, które uzasadniają ingerencję oraz wskazują warunki takiej ingerencji. Co do minimum gwarancji, prawa powinny określać kryteria, na podstawie których można określić osoby potencjalnie dotknięte, powinny zawierać przepisy regulujące dokumentację korzystania z urządzeń wywiadowczych oraz powinny określać zasady dotyczące ochrony oraz niszczenia dokumentacji. Co do podejmowania decyzji w przedmiocie korzystania z urządzeń wywiadowczych, władzom nie może zostać przyznany nadmierny margines uznania (np. *Valenzuela Contreras przeciwko Hiszpanii* (58/1997/842/1048)). Co do stosowania urządzeń wywiadowczych, wymóg ograniczenia dostępu do informacji osobom z zewnątrz stanowi dodatkową gwarancję (np. *Kopp przeciwko Szwajcarii* (13/1997/797/1000) 25 marca 1998).

[74] Użycie w konkretnym celu oznacza, że urządzenia wywiadowcze mogą zostać użyte w celach określonych w artykule 8 ust. 2 .... Zgodność z kryterium konieczności jest ściśle związane z tą kwestią. Podstawowym wymaganiem jest, aby ingerencja była uzasadniona pilnym interesem publicznym i była proporcjonalna zarówno do zagrożenia, któremu należy przeciwdziałać jak i spowodowanych szkód.

[75] Analiza tych kwestii nie powinna ograniczać się do zbadania czy ustawowe warunki określone dla ograniczenia spełniają kryterium proporcjonalności i konieczności, lecz powinna obejmować również analizę konieczności użycia urządzeń wywiadowczych w konkretnej sprawie. Co do wymogu konieczności, nadrzędnym jest, aby każde użycie miało miejsce tylko w wypadku „spotęgowanego” (poważnego) zagrożenia oraz tylko w sprawach, gdzie tradycyjne metody i urządzenia służące do prowadzenia dochodzenia okażą się w danych okolicznościach nieefektywne; ponadto, każdorazowe użycie urządzeń wywiadowczych powinno być stosowane tylko w ścisłej zgodności ze znaną z góry procedurą...

[76] Na podstawie Konwencji i odpowiedniego orzecznictwa Trybunału, Trybunał Konstytucyjny doszedł do wniosku, że bezpieczeństwo narodowe, bezpieczeństwo publiczne oraz ściganie przestępstw, są tego rodzaju interesem, w odniesieniu do którego nawet tajne dochodzenie – które stanowi poważne ograniczenie mechanizmów prawnych – może być stosowane, gdy spełnione są powyższe kryteria.

[77] 3. Trybunał Konstytucyjny przeanalizował kwestionowane przepisy w granicach skargi wniesionej przez skarżących. Skarżący kwestionowali działania organu antyterrorystycznego - gromadzenie danych wywiadowczych, przeprowadzonych w celach innych niż ściganie przestępstw. Podnosili, niezgodność kwestionowanych przepisów z Ustawą Zasadniczą, z tego względu, że pozwalały na gromadzenie danych wywiadowczych na mocy Nbtv. – podczas gdy Nbtv. nie zawierało żadnych gwarancji przestrzegania praw podstawowych.

[78] Skarżący nie dokonali rozróżnienia na różne etapy gromadzenia danych wywiadowczych (zarządzenie, prowadzenie i zakończenie ingerencji), wybrali niektóre elementy stosowania [tego środka] i je skarżyli. Co do zarządzenia ingerencji, zarzucali, że pozwolenie wydane przez Ministra właściwego do spraw sprawiedliwości nie dawało wystarczającej gwarancji, w szczególności ze względu na fakt, że powody stanowiące podstawę żądania udzielenia zezwolenia nie zostały wystarczająco wymienione. Skarżący są zdania, że następujący po zakończeniu ingerencji los informacji niemających znaczenia dla celów inwigilacji oraz los danych odnoszących się osób, których dana sprawa nie dotyczy, nie został uregulowany. ...

[80] W związku z tym, Trybunał Konstytucyjny w granicach zaskarżenia musi przeanalizować, czy zezwolenie wydane organowi antyterrorystycznemu do gromadzenia danych wywiadowczych przez Ministra właściwego do spraw sprawiedliwości oraz czy obsługa danych następująca po zakończeniu ingerencji stanowiła czy też nie stanowiła naruszenia powoływanych praw podstawowych, a mianowicie prawa do prywatności i prawa do autonomii informacyjnej ...

[92] 3.2. Trybunał Konstytucyjny przeanalizował najpierw konstytucyjność wydanego przez Ministra Sprawiedliwości zezwolenia. Pierwszym etapem inwigilacji jest zezwolenie na ingerencję. Ponieważ Minister Sprawiedliwości stosując artykuł 7/E (3) Ustawy o Policji (dalej: Rtv.) i udzielając zezwolenia na korzystanie z urządzeń gromadzenia danych wywiadowczych oraz metod wymienionych w artykule 56 a)-e) Nbtv – zgadza się na ingerencję Państwa, która poważnie narusza prawa podstawowe, to proces ingerencji musi być regulowany prawem, normy prawne muszą być jasne, a proces musi podlegać mechanizmom kontroli zewnętrznej. ...

[94] ... Kwestionowane przepisy Rtv. zezwalają na przeprowadzenie przez organy antyterrorystyczne, w realizowaniu niektórych ze swoich zadań, gromadzenia danych wywiadowczych na mocy Nbtv. Rtv. jasno precyzuje dwa zadania na kanwie, których tajny nadzór może zostać przeprowadzony zgodnie z Nbtv.: mianowicie wykonywanie zadań sprecyzowanych w artykule 7/E (1) a) i ad) oraz w artykule 7/E (1) e).

[95] Zadaniem określonym w artykule 7/E (1) a) (punkcie (ad)), które ma być realizowane w ramach zwalczania terroryzmu, jest zapobieganie, wykrywanie i przeciwdziałanie aktom terroryzmu na terytorium Węgier, w celu wspierania interesów bezpieczeństwa narodowego Węgier. Punkt e) odsyła do punktu d), który zezwala na pozyskiwanie, analizę, ocenę oraz przekazywanie informacji obcemu Państwu lub informacji pochodzących z obcego Państwa, w takim stopniu, w jakim dane te są konieczne do zrealizowania zadania tu określonego. Zadania określone w punkcie d) polegają na uczestniczeniu w ratowaniu, powrocie na Węgry oraz ewakuacji węgierskich obywateli, którzy znaleźli się w kłopotach z powodu działań wojennych lub konfliktów zbrojnych poza terytorium Węgier bezpośrednio zagrażających życiu i ciału obywateli węgierskich lub z powodu ataku terrorystycznego lub pojmania, jako zakładników, jak również dla tych celów na współpracy z Państwami członkowskimi UE, organami Unii Europejskiej, organami Organizacji Traktatu Północnoatlantyckiego, organizacjami międzynarodowymi, których sprawa dotyczy oraz władzami danego Państwa obcego. Zadania te powinny zostać przeprowadzone na mocy decyzji podjętej w tym przedmiocie przez Ministra właściwego do egzekwowania prawa w porozumieniu z Ministrem właściwym do spraw zagranicznych.

[96] Artykuł 7/E (3) Rtv., zakwestionowany przez skarżących, odnoszący się do Nbtv. i powtórzony w Nbtv. stanowi o gromadzeniu danych wywiadowczych (artykuły 53-60) oraz przetwarzaniu pozyskanych danych [artykuły 38-52]. Artykuł 7/E (3) Rtv. przewiduje stosowanie, *mutatis mutandis*, przepisów Nbtv. dotyczących zarówno badania skargi w przedmiocie działań organu antyterrorystycznego jak też badanie sprawozdań zarzucających niezgodne z prawem operacje w ramach działań organu antyterrorystycznego [artykuł 11 (5), artykuł 14 (1)-(2) i (4) a)-f) i (5), artykuł 15 (3), artykuł 16, artykuł 18 oraz artykuł 27 (4) Nbtv.] Ponadto, zakwestionowane przepisy jasno stanowią, że Minister Sprawiedliwości jest uprawniony do wydawania zezwolenia na użycie, w zakresie zadań ustawowych, urządzeń gromadzenia danych wywiadowczych, w przypadkach enumeratywnie wymienionych. W związku z tym, artykuł 7/E (3) Rtv. spełnia wymóg bycia przepisanym przez prawo oraz wymóg przejrzystości norm, gdyż w wystarczający sposób określa warunki zarządzenia środków i ich wykonywania, uregulowanych w Ustawie.

[97] Następnie Trybunał Konstytucyjny zbadał, czy w danej sprawie zezwolenie na gromadzenia danych wywiadowczych przez ministra właściwego do spraw wymiaru sprawiedliwości zapewniło wystarczające gwarancje przestrzegania podstawowych praw jednostek. ...

[102] Gromadzenie danych wywiadowczych dla celów bezpieczeństwa narodowego może mieć miejsce tylko w zgodzie z artykułem 7/E (1) a) ad) lub e) Rtv., to jest w celu zwalczania prób popełnienia aktu terrorystycznego na terytorium Węgier oraz w związku z ochroną obywateli Węgierskich, którzy znaleźli się w kłopotach w obcym kraju. ...

[105] Zakres zadań związanych z bezpieczeństwem narodowym jest znacznie szerszy niż zakres zadań odnoszących się do prowadzenia dochodzeń w konkretnych przestępstwach dla celów bezpieczeństwa narodowego, wydarzenia życia codziennego nie są badane ze względu na ich znaczenie z punktu widzenia prawa karnego, i zdarzenia te nie muszą pociągać za sobą konsekwencji prawnych. Identyfikacja i zwalczanie wysiłków zmierzających do popełnienia czynów mających znaczenie z punktu widzenia zapewnienia suwerenności Państwa oraz ochrony zgodnego z prawem porządku Państwa może wykraczać poza sferę poszczególnych przestępstw. W związku z tym, zadania związane z bezpieczeństwem krajowym nie są porównywalne z gromadzeniem danych wywiadowczych związanym z prowadzonym dochodzeniem w sprawie przestępstw, które jest przeprowadzane zgodnie z artykułem 69 i jest przedmiotem udzielenia zezwolenia przez sąd. Zapobieganie i eliminacja ryzyka dla bezpieczeństwa narodowego wymaga decyzji politycznych, dlatego też decyzje tego typu wchodzą w zakres kompetencji organu wykonawczego. Uzasadnia to uznanie, że generalny charakter gromadzenia informacji wywiadowczych, powinien nastąpić za zgodą Ministra właściwego do spraw wymiaru sprawiedliwości.

[106]Jednakże przy wydawaniu zezwolenia minister właściwy do spraw sprawiedliwości musi wyważyć z jednej strony interes bezpieczeństwa narodowego, a z drugiej szkody wyrządzone prawom podstawowym.W związku z tym, oprócz oceny interesu bezpieczeństwa narodowego kraju pod kątem politycznym (krajowym i zagranicznym), osoba udzielająca zezwolenia powinna również zachować właściwą równowagę między interesami bezpieczeństwa narodowego a prawami podstawowymi.Czyniąc to, należy zacząć od zasady, zgodnie z którą tajne metody wywiadowcze dla celów bezpieczeństwa narodowego mogą być wykorzystywane nawet przez organ antyterrorystyczny jako ostateczny środek wykrywania. Artykuł 53 ust. 2 Nbtv. wyraźnie przewiduje charakter *ultima ratio* metod tajnej inteligencji: specjalne urządzenia i metody tajnego gromadzenia informacji wywiadowczych mogą być stosowane jedynie w przypadku, gdy dane potrzebne do wykonania określonego zadania nie mogą być uzyskane w żaden inny sposób, mianowicie za pomocą tradycyjnych środków wykrywania**.** To postanowienie Nbtv. ma służyć jako gwarancja prawna podobna do tej, która jest określona w przepisach prawach o czynach stanowiących przestępstwa w kontekście gromadzenia danych wywiadowczych związanych z prowadzeniem dochodzenia w sprawie danego przestępstwa i w kontekście podejrzenia popełnienia przestępstwa.

[107] ... Żądanie wydania zezwolenia musi być uzasadnione. Udzielający... zezwolenia opiera swoją decyzję na treści żądania: żądanie zostanie uwzględniona lub w przypadku bezzasadności oddalone. Stąd, gdy wysunięcie żądania przez organ nie może być wystarczająco uzasadnione, że żądane dane służące do wypełnienia przez organ swoich zadań, nie mogą zostać pozyskane w żaden inny sposób, zezwolenie na zastosowanie urządzeń i metod wywiadowczych nie będzie udzielone. ...

[114] W zakresie zarządzenia i przeprowadzenia gromadzenia danych wywiadowczych, zewnętrzna kontrola stanowi fundamentalną gwarancję. Kontrola nad działaniami wykonywanymi przez organ antyterrorystyczny zgodnie z zasadami Nbtv. jest sprawowana przez Parlamentarną Komisję Bezpieczeństwa Narodowego (dalej: Komisja) ... Na wniosek Komisji Minister Sprawiedliwości przedstawi informacje odnoszące się do charakteru udzielonego zezwolenia na gromadzenie danych wywiadowczych oraz kategorii sprawy (artykuł 14(4) b) Nbtv.).

[115] Komisja może uzyskać informacje o nieprawidłowościach związanych z funkcjonowaniem Służb (organów antyterrorystycznych) m. in., z własnych zapytań, skarg obywateli lub informacji otrzymanych od pracowników Służb. ...

[119] Nbtv. ustanawia jedną granicę kontroli Komisji: Komisja nie może uzyskać informacji, które mogłyby zagrozić pierwszorzędnemu interesowi bezpieczeństwa narodowego, tj. ochronie metod i źródeł (uczestniczących osób) powoływanych w rozpatrywanej sprawie (artykuł 16(1) Nbtv.).

[120] Czynności Służb Bezpieczeństwa Narodowego, organu antyterrorystycznego oraz Ministra Sprawiedliwości udzielającego zezwolenia mogą być kontrolowane, oprócz Parlamentu, również przez Parlamentarnego Komisarza ds. Praw Podstawowych.

[121] Zgodnie z artykułem 18 (1) f) Ustawy nr CXI of 2011 o Parlamentarnym Komisarzu ds. Praw Podstawowych (dalej: Ajbt.) organy egzekwowania prawa, w tym organy antyterrorystyczne, mogą zostać sprawdzone przez Rzecznika Praw Obywatelskich. ... Stąd nie istnieją żadne przeszkody do przeprowadzenia kontroli przez rzecznika Praw Obywatelskich, jedyną granicą jest – podobnie jak przy kontroli Parlamentu – wydane sprawozdanie o czynnościach wywiadowczych władz, którym zostało udzielone zezwolenie na korzystanie z urządzeń i metod wywiadowczych - nie może zawierać danych z których można byłoby wnioskować, że organ gromadzi dane wywiadowcze w danej sprawie (artykuł 28(3)). Komisarz ds. Praw Podstawowych może przedstawiać, w przypadku gdy warunki określone w artykule 38 Ajbt. są spełnione, Parlamentowi w corocznym sprawozdaniu, sprawy będące przedmiotem przeprowadzonych przez niego postępowań oraz może, za wyjątkiem wnioskowania o wprowadzenie zmian, żądać od Parlamentu, aby zbadał sprawy. ...

[122] Na podstawie powyższych informacji Trybunał Konstytucyjny skonkludował, że Nbtv. dopuszcza kontrolę zezwolenia udzielonego przez Ministra Sprawiedliwości przez organy niezależne od władzy wykonawczej. ...

[124] 3.3 Analizując odesłanie z artykułu /E (3) Rtv. Trybunał Konstytucyjny zaobserwował, że artykuł 58 (3) Nbtv. nie przewiduje wyraźnego wymogu uzasadniania decyzji....

[127] Element konieczny każdej decyzji podjętej w sprawie gromadzenia danych wywiadowczych, zgodnie z Rtv. polega na kontroli zgodności żądania wydania zezwolenia z ustawowymi wymogami. ...

[128] [...] Odesłanie z artykułu 7/E (3) Rtv. wymaga również wydania przez Ministra Sprawiedliwości zezwolenia na gromadzenie danych wywiadowczych związanych z bezpieczeństwem narodowym prowadzone przez organ antyterrorystyczny, będący częścią Służb Policyjnych, w celu zwalczania prób popełniania aktów terroryzmu na terytorium Węgier lub w związku z ochroną obywateli węgierskich, którzy znaleźli się w kłopotach na terenie obcego kraju. ...

[130] Ponieważ Nbtv. nie wymaga jednoznacznie od Ministra Sprawiedliwości wydania uzasadnionej decyzji, udzielający zezwolenia nie ma obowiązku uzasadniania jej Wobec braku uzasadnienia nie jest jednak możliwe późniejsze zrozumienie, analiza lub kontrola aspektów i powodów dających podstawę do wydania decyzji w konkretnej sprawie, przez tych którzy przeprowadzają zewnętrzną kontrolę.

[131] Choć artykuł 58 (3) Nbtv. stanowi, że udzielając zezwolenia bazuje się na treści żądania, treść ta jest, z definicji, jednostronna, ponieważ twierdząc, że zbieranie danych wywiadowczych jest konieczne, żądanie będzie wyłącznie powoływało się na interes bezpieczeństwa narodowego. Udzielający zezwolenia musi wyważyć interes bezpieczeństwa narodowego i praw podstawowych, zapisanych w artykule VI (1)-(2) Ustawy Zasadniczej, osób dotkniętych przez gromadzenie danych wywiadowczych oraz musi zagwarantować, dodatkowo, że oprócz konieczności ograniczenia, ograniczenie to będzie proporcjonalne. ...

[132] Biorąc pod uwagę, że szczególny charakter inwigilacji wyklucza możliwość zastosowania środka zaradczego, ograniczenie prawa do prywatności i prawa do autonomii informacyjnej, które jest proporcjonalne do ochrony bezpieczeństwa narodowego, będzie wymagało skutecznej kontroli zewnętrznej już przy udzielaniu zezwolenia na stosowanie urządzeń wywiadowczych.

[133] Komisja ds. Bezpieczeństwa Narodowego i Komisarz ds. Praw Podstawowych mogą przeprowadzić efektywną kontrolę zewnętrzną w stosunku do działań podjętych przez Ministra Sprawiedliwości w kwestii wydawania zezwoleń, jeżeli decyzja Ministra zezwalająca na inwigilację zawiera wystarczająco szczegółowe uzasadnienie. Uzasadnienie powinno być tak szczegółowe, aby umożliwić, tym którzy przeprowadzają kontrolę zewnętrzną na wyważenie interesu bezpieczeństwa narodowego i praw podstawowych.

[134] Na podstawie upoważnienia udzielonego w artykule 46 (3) Abtv., w celu zapewnienia skutecznej kontroli zewnętrznej, Trybunał Konstytucyjny określił jako wymóg konstytucyjny zapewnienie zgodności z artykułem VI (1) -(2) Ustawy Zasadniczej, że stosując artykuł 58 (3) Nbtv. decyzja ministra właściwego do spraw wymiaru sprawiedliwości zezwalająca na gromadzenie informacji wywiadowczych musi być poparta uzasadnieniem.

[135] 3.4. W związku z tym Trybunał Konstytucyjny przeanalizował czy przetwarzanie danych przez organ antyterrorystyczny, następujące po zakończeniu zbierania danych wywiadowczych naruszają prawo do autonomii informacyjnej. Skarżący zarzucali, że Nbtv., inaczej niż Rtv., nie przewiduje wymogu usunięcia zgromadzonych danych, które są nieistotne dla celów inwigilacji oraz które są związane z osobami, których sprawa nie dotyczy. ...

[138] Na podstawie powyższych ustaleń Trybunał Konstytucyjny stwierdził, że chociaż Nbtv., w przeciwieństwie do artykułu 73 (3) Rtv., jednoznacznie nie przewiduje wymogu usunięcia zgromadzonych danych, które są nieistotne dla celów inwigilacji oraz które są związane z osobami, których sprawa nie dotyczy, z łącznej interpretacji frazy „oczywiście niepotrzebne” z artykuł 50 (2) e) i artykułu 43 Nbtv. jasno wynika, że wszelkie dane niepotrzebne do osiągnięcia celu służącego za podstawę prawna dla gromadzenia danych, w szczególności dane dotyczących osób, których sprawa nie dotyczy, muszą zostać usunięte z urzędu. Dlatego też powyższa regulacja spełnia zasadę celowości i jest odpowiednia, by zapobiec przechowywaniu danych. Ponadto, Nbtv. pozwala osobom, których dotyczy sprawa na złożenie wniosku o usunięcie swoich danych osobowych, wniosek ten może zostać odrzucony tylko przez dyrektora generalnego z konkretnych powodów. Istnieje również kontrola zewnętrzna nad przetwarzaniem danych, gdyż powody ze względu na które odrzucono żądanie muszą zostać przesłane również do Krajowego Organu ds. Ochrony Danych i Wolności Informacji [artykuł 48 Nbtv.].

[139] W związku z powyższym Trybunał Konstytucyjny oddalił, również w tym zakresie zarzut w zakresie niezgodności kwestionowanego przepisu z Ustawą Zasadniczą, zmierzający do uzyskania stwierdzenia nieważności kwestionowanego przepisu. ...”

III.  EUROPEJSKA KOMISJA NA RZECZ DEMOKRACJI PRZEZ PRAWO („kOMISJA WENECKA”)

21.  Sprawozdanie w sprawie nadzoru demokratycznego nad służbami bezpieczeństwa przyjęte przez Komisję Wenecką na 71. sesji plenarnej (Wenecja, 1‑2 czerwca 2007) (CDL-AD(2007)016-e) zawiera następujące fragmenty:

“81.  Ze względu na znaczenie i charakter przedmiotowych interesów, gromadzenie danych wywiadowczych jest jednym z głównych obszarów krajowych procesów decyzyjnych, w których rząd jest najbardziej niechętny do poddawania się krajowej kontroli legislacyjnej i sądowej, a tym bardziej, międzynarodowemu nadzorowi i kontroli.

82.  Z różnych powodów może dochodzić do napięć w zakresie polityki bezpieczeństwa narodowego, nie tylko między partią rządzącą a opozycją polityczną w danym państwie, ale także napięć konstytucyjnych między władzą wykonawczą a ustawodawczą, napięć w rządzie (zwłaszcza koalicyjnym), napięć między politycznymi przywódcami a personelem wywiadowczym służb ds. bezpieczeństwa. Tworzeniu i operacjom krajowej polityki bezpieczeństwa musi towarzyszyć wysoki stopień tajności. Tajemnica skutkuje jednak również zwiększeniem kontroli rządu nad polityką, kosztem władzy ustawodawczej i izolacją tych pierwszych od krytyki. Sytuację pogarsza fakt, że w dzisiejszych czasach istnieje związek między „zewnętrznymi” i „wewnętrznymi” zagrożeniami dla państwa. W związku z tym informacje dotyczące bezpieczeństwa i informacje wywiadowczych mają tendencję do tworzenia niepodzielnej całości.

86.  W odniesieniu do ograniczonego zakresu kontroli parlamentarnej i sądowej, szczególnie ważne jest zwrócenie uwagi na szczególny charakter wywiadu dotyczącego bezpieczeństwa. Sercem agencji bezpieczeństwa są jej akta wywiadowcze. „Hard” data, tj. informacje czysto rzeczowe, są niewystarczające dla agencji bezpieczeństwa lub organizacji policyjnej. Musi również gromadzić spekulacyjne dane w celu ustalenia, którzy ludzie są lub prawdopodobnie stanowią zagrożenie dla bezpieczeństwa narodowego. Informacje te można uzyskać na różne sposoby. Duża część informacji o bezpieczeństwie wewnętrznym pochodzących z otwartych źródeł pochodzi od informatorów. Podobnie jak informacje oparte na faktach, taka „miękka inwigilacja”, jeżeli służby chcą poprawnie wykonać swoją pracę, może i musi być zestawiona, aby stworzyć profil osobowości podejrzanego lub przeprowadzić analizę podejrzanej działalności. ....

VII. Kontrole wewnętrzne i rządowe jako część ogólnych systemów przejrzystości

130.  Kontrola wewnętrzna służb bezpieczeństwa jest podstawową gwarancją zapobiegania nadużyciom władzy, gdy personel pracujący w służbach jest zaangażowany w demokratyczne wartości państwa i poszanowanie praw człowieka. Kontrole zewnętrzne mają zasadniczo na celu wzmocnienie kontroli wewnętrznych i okresowe zapewnienie ich prawidłowego funkcjonowania.

131.  Kontrole wewnętrzne oznaczają przede wszystkim, że kierownictwo wyższego szczebla służb musi sprawować w praktyce skuteczną kontrolę nad niższymi szczeblami służb.

134.  Podobnie jak silna kontrola wewnętrzna stanowi warunek wstępny skutecznej kontroli wykonawczej nad służbą bezpieczeństwa, tak samo silna kontrola wykonawcza nad służbami bezpieczeństwa jest warunkiem wstępnym odpowiedniej przejrzystości parlamentarnej, gdyż dostęp parlamentu do wywiadu zależy zazwyczaj od władzy wykonawczej. To samo w mniejszym stopniu dotyczy systemów przeglądów eksperckich/autoryzacji, ponieważ mają one własny dostęp do urzędników i materiałów wywiadowczych....

137. W celu zapewnienia rządowi bezstronnej weryfikacji i pewności, że tajne służby działają zgodnie z jego polityką, skutecznie i z zachowaniem należytej staranności, szereg krajów stworzyło biura, takie jak biuro inspektora generalnego, komisarzy sądowniczych lub audytorów, w celu kontrolowania działalności sektora bezpieczeństwa oraz z ustawowymi uprawnieniami w zakresie dostępu do informacji i personelu.

**VIII. Przejrzystość parlamentarna**

150.  Istnieje kilka powodów, dla których parlamentarzyści powinni być zaangażowani w nadzór nad służbami bezpieczeństwa. Po pierwsze, ostateczny autorytet i legitymizacja służb bezpieczeństwa wynika z prawnego zatwierdzenia ich uprawnień, działań i wydatków. Po drugie, istnieje ryzyko, że służby mogą służyć wąskim interesom politycznym, a nie całemu państwu i chronić porządek konstytucyjny, jeżeli demokratyczna kontrola nie obejmuje ich. Stabilne, ponadpartyjne podejście do bezpieczeństwa może zatem zostać zapewnione poprzez odpowiednią kontrolę, z korzyścią dla państwa i samych służb.

153.  Z porównawczej perspektywy międzynarodowej, najczęstszym rozwiązaniem jest ustanowienie przez parlament jednego organu nadzoru dla wszystkich głównych służb bezpieczeństwa i wywiadu, a nie wielu organów nadzoru dla poszczególnych organów.

IX. Kontrola sądowa i wydawanie zezwoleń

195.  Kontrola sądowa nad służbami bezpieczeństwa wewnętrznego może przybierać różne formy. Po pierwsze, w fazie przedprocesowej istnieje wymóg uprzedniej zgody , i/lub po doraźnej kontroli specjalnych środków dochodzeniowych, takich jak podsłuch telefonu, podsłuch i nadzór wideo. W państwach europejskich jest to normalną praktyką.

204.  Niemniej jednak, oczywistą zaletą wymogu uzyskania uprzedniego zezwolenia sądowego w odniesieniu do specjalnych technik dochodzeniowych jest to, że służby bezpieczeństwa muszą wyjść „poza swoje granice” i przekonać niezależną osobę o potrzebie zastosowania określonego środka. Powyższe poddaje kwestie bezpieczeństwa prawu i jako takie służy zinstytucjonalizowaniu poszanowania prawa. Jeżeli system ten będzie działał prawidłowo, zezwolenie sądowe będzie miało skutek prewencyjny, zniechęcający do składania nieuzasadnionych wniosków lub skrócenia czasu trwania specjalnego środka dochodzeniowego. Zgromadzenie Parlamentarne opowiedziało się już wcześniej za uprzednim sądowym zezwoleniem na użycie specjalnych środków dochodzeniowych (w zależności od rodzaju środków).

**X. Przejrzystość organów eksperckich**

218.  Organy eksperckie mogą pełnić funkcję uzupełniającą lub zastępczą dla organów parlamentarnych lub organów wymiaru sprawiedliwości.......

219.  Organ ekspercki jest synonim większej fachowej wiedzy oraz zwiększenia czasu nadzoru nad służbami bezpieczeństwa oraz uniknięcia ryzyka podziałów politycznych oraz „gry” o głosy wyborców, na które komisje parlamentarne mogą być podatne. Organ może sprawować swoją kontrolę w pełnym lub niepełnym wymiarze czasu, nawet jeżeli czas byłby ten niepełny, wykonywany nadzór prawdopodobnie będzie bardziej ciągły niż ten sprawowany przez organ parlamentu, którego członkowie są z różnych partii politycznych i mają inne cele. Kadencja członków może być dłuższa niż standardowa kadencja, coś co jest szczególnie ważne, ponieważ wywiad ma, jak już wspomniano… stosunkowo długą „krzywą uczenia się”.

220. Podobnie jak nadzór parlamentarny, mandat organu eksperckiego może mieć charakter instytucjonalny, co oznacza, że nadzór może być sprawowany jedynie nad określonym organem bezpieczeństwa wewnętrznego (w przeciwieństwie do omówionej poniżej kontroli funkcjonalnej).

222. Ważne jest jednak, aby zakres kontroli był starannie określony, aby uniknąć sporów dotyczących tego, czy dana działalność wchodzi w zakres mandatu organu oraz aby uniknąć nakładania się z innymi mechanizmami przejrzystości, w szczególności kontrolą sądową nad uprawnieniami policyjnymi i odpowiedzialnością ministerialną przed parlamentem..

XI. Mechanizmy dotyczące skarg

241.  Oczywiste jest, że osoby, które twierdzą, że ucierpiały na skutek wyjątkowych uprawnień służb bezpieczeństwa i wywiadu, takich jak nadzór czy poświadczenie bezpieczeństwa, muszą mieć pewne możliwości domagania się zadośćuczynienia. Poza wzmocnieniem przejrzystości, skargi mogą również przyczynić się do poprawy wyników służb poprzez uwypuklenie uchybień administracyjnych. Oczywiście należy również pamiętać o wymogach traktatów dotyczących praw człowieka, a zwłaszcza Europejskiej Konwencji Praw Człowieka, wraz z ochroną sprawiedliwego procesu, poszanowania życia prywatnego i wymogu skutecznego środka prawnego.

242.  Z oczywistych względów, pomimo uprawnionych celów służby bezpieczeństwa lub wywiadu nie powinny mieć możliwości korzystania z systemu skarg w celu uzyskania informacji o pracy służb. System skarg powinien zapewniać równowagę między niezależnością, solidnością i uczciwością z jednej strony, a wrażliwością na potrzeby bezpieczeństwa z drugiej. Stworzenie takiego systemu jest trudne, ale nie niemożliwe.

243.  Jednostki, które zarzucają Państwu popełnienie przestępstw z innej dziedziny, mają rutynowo prawo do dochodzenia odszkodowania przed sądem. Skuteczność tego prawa zależy jednak od wiedzy jednostki o zarzucanym czynie bezprawnym oraz przedstawienia dowodu na tę okoliczność. Jak już wspomniano, z różnych powodów zdolność sądów powszechnych do zapewnienia odpowiedniego środka odwoławczego w dziedzinie bezpieczeństwa jest ograniczona. Orzecznictwo Europejskiego Trybunału Praw Człowieka.... bardzo wyraźnie stwierdza, że środek zaradczy nie może być tylko dostępny na papierze.

244.  Alternatywą jest zezwolenie na przeprowadzenie dochodzenia i złożenie skargi na działania służb przez niezależnego urzędnika, takiego jak Rzecznik Praw Obywatelskich....

245.  W systemach tego typu (z Rzecznikiem Praw Obywatelskich) kładzie się nacisk na niezależne dochodzenie prowadzone przez urzędnika w imieniu skarżącego. Te niezależne urzędy zazwyczaj istnieją po to, by poradzić sobie z administracyjną porażką organów publicznych, a nie z błędem prawnym. Ich dochodzenia mogą kłaść mniejszy nacisk na własny udział skarżącego w procesie i przejrzystość niż w przypadku postępowania sądowego. Zazwyczaj tego rodzaju dochodzenie nie kończy się wyrokiem i możliwością wniesienia środków odwoławczych, lecz sprawozdaniem, a (jeżeli skarga zostanie podtrzymana) zaleceniem naprawienia sytuacji i podjęcia działań w przyszłości...

246.  Mniej powszechną opcją jest sytuacja, w której państwo korzysta z parlamentarnego lub eksperckiego organu nadzoru w celu rozpatrywania skarg i zażaleń jednostek...... Parlamentarny organ nadzorczy może odnieść korzyści w zakresie rozpatrywania skarg wniesionych przeciwko służbom bezpieczeństwa i wywiadu, ponieważ umożliwi to wgląd w potencjalne niepowodzenia - w zakresie polityki, legalności i skuteczności. Z drugiej strony, jeżeli organ nadzoru jest zbyt ściśle powiązany ze służbami, które nadzoruje lub działa w ramach tajemnicy, skarżący może mieć poczucie, że proces rozpatrywania skarg nie jest wystarczająco niezależny. W przypadkach, w których jeden organ rozpatruje skargi i sprawuje nadzór, najlepiej byłoby, gdyby istniały całkiem odrębne procedury prawne dla tych różnych ról.

247.  Ogólnie rzecz biorąc, lepiej jest powierzyć te dwie funkcje różnym organom, ale należy wprowadzić odpowiednie procedury, aby organ nadzoru był świadomy szerszych konsekwencji poszczególnych skarg. Podejście to popiera również Europejski Trybunał Praw Człowieka. Wymóg zawarty w art. 13 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności dotyczący mechanizmu odwoławczego w przypadku domniemanego naruszenia praw wynikających z Konwencji, który jest niezależny od procesu autoryzacji, oznacza, że system kontroli państwa, np. w przypadku przetwarzania danych, może zdać test „zgodności z prawem” i „konieczności w społeczeństwie demokratycznym”, ale pomimo tego brak środków zaradczych oznacza naruszenie konwencji. Jak już wspomniano, ETPCz stwierdził, że środek odwoławczy musi być skuteczny pod względem prawnym i faktycznym. Należy w szczególności zauważyć, że Europejski Trybunał Praw Człowieka orzekł, że niezależny organ nadzorujący dane, który posiada formalne kompetencje prawne w zakresie przyznawania środków zaradczych w odniesieniu do przechowywania niedokładnych, nieodpowiednich itp. danych dotyczących bezpieczeństwa, ale który w rzeczywistości nie posiada wiedzy specjalistycznej niezbędnej do oceny tych danych, nie jest skutecznym środkiem zaradczym w rozumieniu art. 13.

249.  W niektórych krajach nie tylko osoby fizyczne, ale również członkowie służb mogą zwracać uwagę Rzecznika Praw Obywatelskich lub parlamentarnego organu nadzorczego na kwestie związane z działaniami służb...

250.  Inną metodą rozpatrywania skarg jest powoływanie wyspecjalizowanego sądu.”

IV.  INNE STOSOWNE TEKSTY MIĘDZYNARODOWE

22.  Kilka istotnych, w niniejszym kontekście, elementów prawa międzynarodowego zostało przedstawionych w sprawie *Dragojević przeciwko Chorwacji* (nr 68955/11, §§ 62 do 66, 15 stycznia 2015).

23.  W *Digital Rights Ireland przeciwko Minister for Communications i In.*, (sprawy: C-293/12 oraz C-594/12, 8 kwietnia 2014), Europejski Trybunał Sprawiedliwości orzekł następująco:

“26.  W tym względzie należy zwrócić uwagę, że danymi, do których zatrzymywania zobowiązani są – na podstawie art. 3 i 5 dyrektywy 2006/24 – dostawcy ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności, są w szczególności dane niezbędne do ustalenia źródła oraz odbiorcy połączenia, do określenia daty, godziny i czasu trwania połączenia oraz jej rodzaju, do określenia narzędzia komunikacji i do identyfikacji lokalizacji urządzenia komunikacji ruchomej, w tym między innymi nazwiska i adresu abonenta lub zarejestrowanego użytkownika, numeru nadawcy i odbiorcy połączenia, a także adresu IP w przypadku usług internetowych. Dane te pozwalają w szczególności ustalić, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik, a także – czas połączenia oraz miejsce, z którego zostało ono nawiązane. Dzięki nim można też ustalić częstotliwości komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie..

27.  Całokształt tych danych może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają..

...

52.  Co się tyczy prawa do poszanowania życia prywatnego, zgodnie z utrwalonym orzecznictwem ochrona tego prawa podstawowego w każdym wypadku wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne (wyrok IPI, C‑473/12, [EU:C:2013:715](http://eur-lex.europa.eu/legal-content/redirect/?urn=ecli:ECLI%3AEU%3AC%3A2013%3A715&lang=PL&format=pdf&target=CourtTab" \t "CourtTab), pkt. 39 i przytoczone tam orzecznictwo).

62.  W szczególności dyrektywa 2006/24 nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby ograniczyć liczbę osób uprawnionych do uzyskiwania dostępu i późniejszego wykorzystywania zatrzymanych danych do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu. Przede wszystkim to uzyskanie przez właściwe organy krajowe dostępu do danych nie podlega uprzedniej kontroli sądu lub niezależnego organu administracyjnego, które pilnowałyby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu, oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw. Co więcej, dyrektywa nie nakazuje państwom członkowskim w sposób wyraźny ustanowienia takich mechanizmów.”

24.  Sprawozdanie z 2013 roku specjalnego sprawozdawcy Organizacji Narodów Zjednoczonych w sprawie propagowania i ochrony prawa do wolności poglądów i wypowiedzi, Franka la Rue, zawiera następujące konkluzje i rekomendacje:

“78.  Techniki i technologie łączności znacznie się rozwinęły, zmieniając sposób prowadzenia nadzoru łączności przez państwa. Państwa muszą zatem uaktualniać swoje rozumienie i regulację nadzoru łączności oraz modyfikować swoje praktyki w celu zapewnienia poszanowania i ochrony praw człowieka.

79.  Państwa nie mogą zagwarantować, że jednostki będą mogły swobodnie poszukiwać i otrzymywać informacje lub wyrażać się bez poszanowania, ochrony i promowania ich prawa do prywatności. Prywatność i wolność wypowiedzi są ze sobą powiązane i wzajemnie zależne; naruszenie jednej z nich, może być zarówno przyczyną, jak i konsekwencją naruszenia drugiej. Na przykład bez odpowiedniego prawodawstwa i norm prawnych zapewniających prywatność, bezpieczeństwo i anonimowość komunikacji, dziennikarze, obrońcy praw człowieka i osoby zgłaszające przypadki naruszenia nie mogą mieć pewności, że ich porozumiewanie się nie będzie podlegało kontroli państw członkowskich.

80.  Aby wypełnić swoje zobowiązania w zakresie praw człowieka, państwa członkowskie muszą zapewnić, aby prawo do wolności wypowiedzi i prywatności było centralnym elementem ram nadzoru łączności. W tym celu Specjalny Sprawozdawca zaleca, co następuje:

**A.  Aktualizacja i wzmocnienie przepisów i standardów prawnych**

81. Nadzór łączności powinien być uważany za działanie wysoce inwazyjne, które potencjalnie narusza prawo do wolności wypowiedzi i prywatności oraz zagraża fundamentom społeczeństwa demokratycznego. Prawodawstwo musi stanowić, że nadzór Państwa nad korespondencją musi mieć miejsce jedynie w najbardziej wyjątkowych okolicznościach i wyłącznie pod nadzorem niezależnego organu sądowego. Środki zabezpieczające muszą być określone w przepisach prawnych odnoszących się do charakteru, zakresu i czasu trwania możliwych środków, podstaw ich zarządzenia, organów właściwych do ich zatwierdzania, wykonywania i nadzorowania oraz rodzaju środków zaradczych przewidzianych w prawie krajowym.

82.  Jednostki powinny mieć prawo do otrzymania powiadomienia, że zostały poddane nadzorowi łączności lub że Państwo miało dostęp do ich danych dotyczących łączności. Uznając, że wcześniejsze lub równoczesne powiadamianie może zagrozić skuteczności nadzoru, jednostki powinny być jednak powiadamiane po zakończeniu nadzoru i powinny mieć możliwość dochodzenia zadośćuczynienia w odniesieniu do stosowania środków nadzoru łączności po jego zakończeniu.

83.  Ramy prawne muszą zapewniać, że środki nadzoru łączności:

(a)  są określone przepisami prawa, spełniającymi wymogi jasności i precyzji, które wystarczają do zapewnienia, że jednostki zostały uprzednio powiadomione i można przewidzieć ich stosowanie;

(b)  są ściśle i wyraźnie konieczne do osiągnięcia zgodnego z prawem celu; oraz

(c)  są dostosowane do zasady proporcjonalności, a gdy dostępne są techniki mniej inwazyjne lub gdy nie zostały jeszcze wyczerpane, nie są stosowane.

84.  Państwa powinny kryminalizować nielegalną inwigilację ze strony podmiotów publicznych lub prywatnych. Przepisy prawne nie mogą być wykorzystywane w odniesieniu do osób zgłaszających przypadki naruszenia praw człowieka lub innych osób usiłujących ujawnić takie przypadki łamania praw człowieka, nie powinny też utrudniać uzasadnionej kontroli działań rządu przez obywateli.

85.  Przekazywanie Państwom danych dotyczących łączności przez sektor prywatny powinno być wystarczająco uregulowane, aby zapewnić, że prawa człowieka jednostek są zawsze traktowane priorytetowo. Dostępu do danych dotyczących łączności przechowywanych przez krajowe podmioty korporacyjne należy poszukiwać wyłącznie w okolicznościach, w których wyczerpane zostały inne dostępne, mniej inwazyjne techniki.

86.  Przekazywanie Państwu danych dotyczących komunikacji powinno być monitorowane przez niezależny organ, taki jak sąd lub mechanizm nadzorujący. Na szczeblu międzynarodowym państwa powinny przyjąć traktaty o wzajemnej pomocy prawnej w celu uregulowania dostępu do danych dotyczących łączności będących w posiadaniu zagranicznych podmiotów korporacyjnych.

87.  Techniki i praktyki nadzoru stosowane poza granicami państwa prawa muszą podlegać kontroli legislacyjnej. Ich pozaprawne stosowanie podważa podstawowe zasady demokracji i może mieć szkodliwe skutki polityczne i społeczne.

**B.  Ułatwienie komunikacji prywatnej, bezpieczeństwa komunikowania się oraz anonimowego komunikowania się**

88.  Państwa powinny powstrzymać się od identyfikacji użytkowników jako warunku koniecznego dostępu do łączności, w tym usług internetowych, kafejek internetowych i telefonii komórkowej..

89.  Jednostki powinny mieć swobodę korzystania z dowolnie wybranej przez siebie technologii w celu zabezpieczenia komunikacji. Państwa nie powinny ingerować w korzystanie z technologii szyfrowania ani zmuszać do udostępniania kluczy szyfrujących.

90.  Państwa nie powinny zatrzymywać lub wymagać zatrzymywania określonych informacji wyłącznie do celów nadzoru.

**C.  Zwiększenie publicznego dostępu do informacji, zrozumienie i świadomość zagrożeń dla prywatności**

91.  Państwa powinny działać całkowicie przejrzyście w stosowaniu i w zakresie technik i uprawnień nadzoru łączności. Powinny one co najmniej publikować zbiorcze informacje na temat liczby zatwierdzonych i odrzuconych wniosków, podziale wniosków na usługodawcę oraz na dochodzenia i jego cel.

92.  Państwa powinny dostarczyć jednostkom wystarczające informacje umożliwiające im pełne zrozumienie zakresu, charakteru i stosowania przepisów prawnych zezwalających na nadzór łączności. Państwa powinny umożliwić dostawcom usług publikowanie stosowanych przez nich procedur nadzoru łączności państwowej, przestrzeganie tych procedur i publikowanie rejestrów nadzoru łączności państwowej.

93.  Państwa powinny ustanowić niezależne mechanizmy nadzoru mogące zapewnić przejrzystość i transparentność nadzoru państwa nad komunikacją.

94.  Państwa powinny podnosić świadomość społeczną w zakresie stosowania nowych technologii komunikacyjnych w celu wspierania jednostek w prawidłowej ocenie, zarządzaniu, ograniczaniu i podejmowaniu świadomych decyzji dotyczących ryzyka związanego z komunikacją.

**D.  Regulacja komercjalizacji technologii nadzoru**

95.  Państwa powinny dopilnować, aby dane dotyczące łączności gromadzone przez podmioty korporacyjne przy świadczeniu usług łączności spełniały najwyższe standardy ochrony danych.

96.  Państwa muszą powstrzymać się od zmuszania sektora prywatnego do wdrażania środków zagrażających prywatności, bezpieczeństwu i anonimowości usług łączności, w tym wymogu stworzenia możliwości przechwytywania danych do celów nadzoru państwa lub zakazu stosowania szyfrowania.

97.  Państwa muszą podjąć środki zapobiegające komercjalizacji technologii nadzoru, zwracając szczególną uwagę na badania, rozwój, handel, eksport i wykorzystanie tych technologii, biorąc pod uwagę ich zdolność do ułatwiania systematycznego łamania praw człowieka.

**E.  Kontynuacja oceny istotnych międzynarodowych zobowiązań w zakresie praw człowieka**

98.  Istnieje znacząca potrzeba pogłębiania międzynarodowego zrozumienia kwestii ochrony prawa do prywatności w świetle postępu technologicznego. Komitet Praw Człowieka powinien rozważyć możliwość wydania nowego komentarza ogólnego w sprawie prawa do prywatności, który zastąpi komentarz ogólny nr 16 (1988).

99.  Mechanizmy dotyczące praw człowieka powinny dodatkowo oceniać obowiązki podmiotów prywatnych opracowujących i dostarczających technologie nadzoru "

25.  Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez amerykańskie NSA programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, zawiera następujące fragmenty:

Wpływ masowej inwigilacji

“...

G. mając na uwadze, że od czerwca 2013 r. wspomniane doniesienia wywołały w UE liczne obawy dotyczące: ...

- możliwości wykorzystywania masowej inwigilacji w celach niezwiązanych z bezpieczeństwem narodowym i bezpośrednią walką z terroryzmem, np. szpiegostwo gospodarcze i przemysłowe lub profilowanie pod względem przekonań politycznych;

- podważania wolności prasy i komunikacji przedstawicieli zawodów, których obowiązuje tajemnica zawodowa, w tym prawników i lekarzy;

- odnośnych ról oraz stopnia zaangażowania agencji wywiadu oraz prywatnych spółek informatycznych i telekomunikacyjnych;

- coraz bardziej zacierających się granic między egzekwowaniem prawa a działaniami wywiadowczymi, co prowadzi do traktowania każdego obywatela jako osoby podejrzanej i obejmowania go nadzorem;

- zagrożenia prywatności w erze cyfrowej i oddziaływanie masowego nadzoru na obywateli i społeczeństwa;

...

T.  mając na uwadze, że prawa podstawowe, szczególnie wolność wypowiedzi, prasy, myśli, sumienia, wyznania oraz wolność zrzeszania się, prawo do prywatności, ochrona danych osobowych, a także prawo do skutecznego środka odwoławczego, domniemanie niewinności oraz prawo do rzetelnego procesu sądowego i brak dyskryminacji, zapisane w Karcie praw podstawowych Unii Europejskiej oraz europejskiej konwencji praw człowieka, stanowią podwaliny demokracji; mając na uwadze, że prowadzenie na masową skalę nadzoru nad ludźmi nie jest spójne z tymi fundamentami;

...

Demokratyczny nadzór nad służbami wywiadowczymi

BW. mając na uwadze, że służbom wywiadowczym w społeczeństwach demokratycznych udzielono specjalnych uprawnień i zapewniono im możliwości ochrony praw podstawowych, demokracji oraz rządów prawa, praw obywateli i Państwa przed poważnymi zagrożeniami wewnętrznymi i zewnętrznymi, podlegają one również kontroli sądowej oraz rozliczalności demokratycznej; mając na uwadze, że służby te dysponują szczególnymi uprawnieniami i możliwościami wyłącznie w tym zakresie; mając na uwadze, że uprawnienia te powinny być wykorzystywane w ramach granic prawnych wyznaczonych prawami podstawowymi, demokracją i praworządnością, zaś ich stosowanie powinno podlegać skrupulatnej kontroli, w przeciwnym wypadku służby tracą legitymizację oraz ryzykują podważeniem demokracji;

BX. mając na uwadze fakt, że dozwolony jest pewien stopień poufności w przypadku służb wywiadowczych z uwagi na potrzebę uniknięcia narażania prowadzonych operacji, ujawnienia trybu funkcjonowania służb lub zagrożenia życia agentów, przy czym poufność taka nie może być nadrzędna w stosunku do zasad demokratycznej i sądowej kontroli i inspekcji ich działalności, jak również przejrzystości lub ich wyłączać, szczególnie jeżeli chodzi o poszanowanie praw podstawowych i praworządności, które stanowią podwaliny społeczeństwa demokratycznego;

BY. mając na uwadze, że większość istniejących krajowych mechanizmów oraz organów nadzoru utworzono lub zrekonstruowano w latach 90. XX w. i niekoniecznie przystosowano je do gwałtownego rozwoju politycznego i technologicznego, jaki można było zaobserwować w ostatnim dziesięcioleciu, a który doprowadził do aktywniejszej międzynarodowej współpracy wywiadu, która obejmuje także wymianę danych osobowych na wielką skalę, jak również do zatarcia granicy dzielącej wywiad i działania w zakresie egzekwowania prawa;

BZ.  mając na uwadze, że demokratyczny nadzór nad działaniami wywiadowczymi jest w dalszym ciągu prowadzony wyłącznie na szczeblu krajowym, pomimo rosnącej wymiany informacji między państwami członkowskimi UE oraz między Państwami Członkowskimi a państwami trzecimi; mając na uwadze, że istnieje coraz większa przepaść między poziomem międzynarodowej współpracy a możliwościami nadzoru ograniczonymi do szczebla krajowego, co skutkuje niewystarczającą i nieskuteczną kontrolą demokratyczną;

CA. mając na uwadze, że krajowe organy nadzoru często nie mają pełnego dostępu do informacji otrzymywanych od zagranicznej agencji wywiadu, co może prowadzić do luk, w których międzynarodowa wymiana informacji może odbywać się bez adekwatnej kontroli; mając na uwadze, że problem ten dodatkowo pogłębia tzw. zasada osoby trzeciej lub zasada kontroli organu zastrzegającego, opracowana z myślą o umożliwieniu organowi zastrzegającemu sprawowania kontroli nad dalszym rozpowszechnianiem należących do niego szczególnie chronionych danych, która to zasada jest jednak niestety często rozumiana jako mająca zastosowanie również do kontroli służb odbiorcy;

CB. mając na uwadze, że prywatne i publiczne inicjatywy reformatorskie na rzecz przejrzystości są kluczowe dla zapewnienia publicznego zaufania do działań agencji wywiadu; mając również na uwadze, że systemy prawne nie powinny uniemożliwiać przedsiębiorstwom ujawniania opinii publicznej informacji na temat sposobu reagowania na wszelkiego rodzaju wnioski rządowe oraz nakazy sądowe dotyczące dostępu do danych użytkownika, w tym możliwości ujawniania zbiorczych zestawień dotyczących liczby wniosków i nakazów w podziale na zrealizowane i odrzucone;

Główne ustalenia

...

6.  przypomina zdecydowane przekonanie UE o konieczności znalezienia równowagi między środkami bezpieczeństwa a ochroną wolności obywatelskich i praw podstawowych, przy jednoczesnym zapewnieniu jak największego poszanowania prywatności i ochrony danych;

7.  uważa, że gromadzenie danych na taką skalę wzbudza znaczne wątpliwości, czy jest ono faktycznie motywowane wyłącznie walką z terroryzmem, ponieważ gromadzeniu podlegają wszelkie możliwe dane na temat wszystkich obywateli; wskazuje zatem na możliwość istnienia innych celów, w tym szpiegostwa politycznego i gospodarczego, którą należy wyeliminować;

8.  kwestionuje zgodność działań w zakresie szpiegostwa gospodarczego prowadzonych na masową skalę przez niektóre państwa członkowskie z unijnymi przepisami dotyczącymi rynku wewnętrznego i konkurencji zapisanymi w tytule I oraz tytule VII Traktatu o funkcjonowaniu Unii Europejskiej; potwierdza zasadę lojalnej współpracy zapisaną w art. 4 ust. 3 Traktatu o Unii Europejskiej, oraz zasadę, w myśl której państwa członkowskie „powstrzymują się od podejmowania wszelkich środków, które mogłyby zagrażać urzeczywistnieniu celów Unii”;

10.   potępia zakrojone na szeroką skalę, regularne i nieograniczone gromadzenie danych niewinnych osób, często zawierających informacje o bardzo osobistym charakterze; podkreśla, że systemy masowego i nieograniczonego nadzoru prowadzonego przez służby wywiadowcze stanowią poważną ingerencję w prawa podstawowe obywateli; podkreśla, że prywatność nie jest luksusem, ale fundamentem wolnego i demokratycznego społeczeństwa; wskazuje ponadto, że prowadzony na masową skalę nadzór ma potencjalnie poważny wpływ na wolność prasy, myśli i słowa oraz na wolność zrzeszania się i zgromadzeń, a także wiąże się z istotną możliwością niewłaściwego wykorzystywania zgromadzonych informacji przeciwko przeciwnikom politycznym; podkreśla, że działalność w zakresie masowego nadzoru obejmuje również prowadzenie przez służby wywiadowcze działań niezgodnych z prawem i rodzi pytanie o eksterytorialność przepisów krajowych;

12.  postrzega programy nadzoru jako kolejny krok w kierunku stworzenia w pełni prewencyjnego państwa, w którym zmianie ulegnie utrwalony w państwach demokratycznych paradygmat prawa karnego, wskutek czego jakakolwiek ingerencja w prawa podstawowe podejrzanych wymagać będzie zatwierdzenia przez sędziego lub prokuratora na podstawie racjonalnego podejrzenia i uregulowania prawnie, natomiast promowane będzie połączenie egzekwowania prawa i działań wywiadowczych o zatartych i osłabionych zabezpieczeniach prawnych, często niezgodne z kontrolą i równowagą demokratyczną oraz prawami podstawowymi, szczególnie w kwestii domniemania niewinności; przywołuje w związku z tym orzeczenie niemieckiego Federalnego Trybunału Konstytucyjnego w sprawie zakazu stosowania siatek prewencyjnych (‘*präventive Rasterfahndung*’) w sytuacji braku dowodu istnienia konkretnego zagrożenia dla innych, ważnych chronionych przepisami praw, z którego to orzeczenia wynika, że ogólna sytuacja zagrożenia lub napięcia międzynarodowe nie są wystarczającym uzasadnieniem dla stosowania tego typu środków;;

...

14.  uznaje, że powyższe niepokoje pogłębia szybki rozwój techniki oraz społeczeństwa, jako że internet i urządzenia przenośne są wszechobecne we współczesnym życiu codziennym (wszechobecna informatyzacja), a model biznesowy większości przedsiębiorstw internetowych opiera się na przetwarzaniu danych osobowych; uważa, że skala tego problemu nie ma precedensu; zwraca uwagę, że może to przyczyniać się do powstania sytuacji nadużywania infrastruktury do masowego gromadzenia i przetwarzania danych w przypadkach zmiany systemu politycznego; ...”

PRAWO

I.  DOMNIEMANE NARUSZENIE ARTYKUŁU 8 KONWENCJI

26.  Skarżący zarzucali, na podstawie art. 8 Konwencji, że mogą potencjalnie podlegać środkom z „artykułu 7/E (3) inwigilacja”. Twierdzili, że uregulowania prawne były podatne na nadużycia, zwłaszcza z powodu braku kontroli sądowej.

Artykuł 8 stanowi, jak następuje:

“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 innych osób.”

27.  Rząd zakwestionował te zarzuty.

A.  Dopuszczalność

1.  Stanowiska stron

28.  Rząd formalnie nie zakwestionował statusu potencjalnych ofiar skarżących w rozumieniu orzecznictwa Trybunału, zgodnie z którym samo istnienie aktu prawnego pozwalającego na użycie urządzeń wywiadowczych służyło jako podstawa do przyznania statusu ofiary, nawet jeżeli nigdy nie użyto takiego urządzenia w stosunku do skarżącego. Jednakże Rząd zakwestionował zarzuty skarżących, jakoby - jako pracownicy organizacji „strażniczej”- byli oni bezpośrednio dotknięci w większym stopniu niż inni możliwością bycia poddanym nadzorowi.

29.  Ponadto Rząd stwierdził, że w skardze konstytucyjnej skarżący nie skarżyli się na obecność lub brak gwarancji w całym procesie gromadzenia danych wywiadowczych. Ich skarga dotyczyła jedynie zezwolenia Ministra Sprawiedliwości na ingerencję oraz przetwarzanie danych po ustaniu ingerencji. Rząd podkreślił, że w odniesieniu do wszelkich dalszych skarg, jakie skarżące mogą mieć w związku z innymi etapami postępowania, nie wyczerpali oni dostępnych krajowych środków odwoławczych.

30.  W odniesieniu do statusu ofiary skarżący podkreślali, że brak znaczącej kontroli zewnętrznej nad wykorzystywaniem tajnego nadzoru zagrażał prywatności jednostek, ponieważ nic nie przeszkadzało władzy politycznej w arbitralnym korzystaniu z tej prerogatywy. Działalność „strażnicza” nie może służyć jako podstawa do tajnego gromadzenia informacji wywiadowczych. Niemniej ich oświadczenie, zgodnie z którym oni, jako pracownicy organizacji strażniczych krytykujących Rząd, czuli się bardziej sfrustrowani i zaniepokojeni tajnym nadzorem niż prawdopodobnie przeciętni obywatele - nie mogło być postrzegane jako strach oparty na całkowicie nieuzasadnionych założeniach, zwłaszcza jeżeli uznać niektóre z niedawnych działań rządu za skierowane przeciwko organizacjom obywatelskim.

31.  W odniesieniu do wyczerpania krajowych środków odwoławczych, skarżący nie zaprzeczali, że ich skarga konstytucyjna koncentrowała się na systemie zezwoleń, ponieważ jedynie zabezpieczenia wprowadzone na tym etapie były w stanie zapewnić odpowiednią ochronę prawa do prywatności. Oznaczało to, że gwarancje związane z późniejszymi etapami postępowania nie były w stanie zrównoważyć szkody wyrządzonej prawu do prywatności, jeżeli nie istniał żaden mechanizm kontroli wbudowany w proces autoryzacji tajnego nadzoru, który mógłby utrudniać prawnie nieuzasadnione interwencje w sferę prywatną. Jednakże pytanie, czy twierdzenie to było prawidłowe, można by ocenić jedynie biorąc pod uwagę całą procedurę. Sugestia rządu, zgodnie z którą Trybunał powinien powstrzymać się od oceny etapów postępowania po zakończeniu fazy udzielania zezwoleń była bezprzedmiotowa i praktycznie niewykonalna. Skarżący podkreślali ponadto, że skarga konstytucyjna złożona do Trybunału Konstytucyjnego oraz skarga złożone do Trybunału w pełni nie odpowiadają sobie nawzajem pod względem przedstawionych argumentów i że w związku z tym Trybunał nie powinien powstrzymywać się, opierając się wyłącznie na zasadzie pomocniczości, od zbadania kwestii, czy pozostałe gwarancje udzielone w ramach procedury zapewniają odpowiednią ochronę.

2.  Ocena Trybunału

32.  Co się tyczy statusu skarżących jako ofiary, Trybunał konsekwentnie orzekał w swoim orzecznictwie, że jego zadaniem nie jest zwykle przegląd prawa i praktyki w abstrakcyjny sposób, lecz ustalenie, czy sposób, w jaki zostały one zastosowane lub naruszone, doprowadził do naruszenia Konwencji. (zobacz, *inter alia*, *Klass i Inni przeciwko Niemcom*, 6 września 1978, § 33, Seria A nr 28; *N.C. przeciwko Włochom* [WI], nr 24952/94, § 56, ETPCz 2002‑X; oraz *Krone Verlag GmbH & Co. KG przeciwko Austrii* (nr 4), nr 72331/01, § 26, 9 listopada 2006).

33 Jednakże, uznając szczególne cechy środków nadzoru oraz znaczenie zapewnienia skutecznej kontroli i nadzoru nad nimi, Trybunał uznał, że w pewnych okolicznościach dana osoba może powołać się na fakt, że jest ofiarą samego istnienia przepisów zezwalających na niejawny nadzór, nawet jeżeli nie może wskazać konkretnych środków, które jej konkretnie dotyczą. Podejście Trybunału do oceny, czy miała miejsce ingerencja w sprawach podnoszących kwestię dotyczącą prawodawstwa pozwalającego na stosowanie tajnych środków nadzoru, zostało przedstawione w wyroku *Klass i Inni* (cytowany powyżej, §§ 34 and 36) następująco:

 “34.  ... skuteczność (*l’effet utile*) Konwencji implikuje, w takich okolicznościach możliwość uzyskania dostępu do Komisji. Gdyby tak nie było, skuteczność mechanizmów egzekwowania Konwencji zostałaby znacznie osłabiona. Zważywszy na fakt, że Konwencja i jej instytucje zostały powołane w celu ochrony jednostki, postanowienia proceduralne Konwencji muszą być stosowane w taki sposób, aby system indywidualnych skarg był skuteczny.

Trybunał uznał zatem, że jednostka może pod pewnymi warunkami powołać się na to, że padła ofiarą naruszenia spowodowanego samym istnieniem tajnych środków lub przepisów dopuszczających tajne środki, bez konieczności zarzucania, że środki te zostały wobec niej faktycznie zastosowane. Odpowiednie warunki powinny być każdorazowo ustalane zgodnie z prawem lub prawami, co do których istnieje domniemanie naruszenia Konwencji, tajnym charakterem kwestionowanych środków oraz związkiem między skarżącym a tymi środkami.

...

36.  Trybunał przypomniał, że w przypadku gdy Państwo ustanawia nadzór, którego istnienie nie jest znane kontrolowanym osobom, co powoduje, że nadzór nie może zostać podważony, art. 8 może zostać w znacznym stopniu ograniczony lub zniesiony. W takiej sytuacji możliwe jest, aby osoba fizyczna była traktowana w sposób sprzeczny z art. 8 lub nawet została pozbawiona prawa przyznanego na mocy tego artykułu nie wiedząc o tym, bez możliwości uzyskania przez nią środków zaradczych ani na szczeblu krajowym, ani przed instytucjami Konwencji.. ...

Trybunał uznał za niedopuszczalne, że pozbawienie gwarancji korzystania z prawa zagwarantowanego przez Konwencję może zostać tym samym unieważnione przez sam fakt, że dana osoba nie jest świadoma jego naruszenia. Prawo odwołania się do Komisji w odniesieniu do osób, na które może mieć wpływ nadzór tajny, wynika z art. 25, ponieważ w przeciwnym razie istnieje ryzyko zniesienia art. 8..”

34. Podążając za wyrokami w sprawach *Klass i Inni* (cytowany powyżej) oraz *Malone przeciwko Zjednoczonemu Królestwu* (2 sierpnia 1984, § 64, Seria A nr 82), poprzednia Komisja, w szeregu spraw przeciwko Zjednoczonemu Królestwu, w których skarżący zarzucali faktyczne przechwycenie ich korespondencji, podkreśliła, że test z *Klass i Inni* nie może być interpretowany tak szeroko, aby obejmował każdą osobę w Zjednoczonym Królestwie, która obawiała się, że służby bezpieczeństwa mogły sprawować nad nią nadzór. W związku z tym Komisja wymagała od skarżących wykazania, że istnieje „uzasadnione prawdopodobieństwo”, iż środki zostały zastosowane wobec nich (zobacz, na przykład, *Esbester przeciwko Wielkiej Brytanii*, nr 18601/91, decyzja Komisji z dnia 2 kwietnia 1993; *Redgrave przeciwko Zjednoczonemu Królestwu*, nr 20271/92, decyzja Komisji z 1 września 1993; oraz *Matthews przeciwko Wielkiej Brytanii*, nr 28576/95, decyzja Komisji z dnia 16 października 1996); konsekwentnie, Trybunał zastosował to samo podejście (zobacz *Halford przeciwko Zjednoczonemu Królestwu*, 25 czerwca 1997, §§ 56 do 57, *Sprawozdania z Wyroków i Decyzji* 1997‑III).

35.  W odniesieniu do niniejszej skargi w sposób bardziej trafny, w innych sprawach dotyczących skarg odnoszących się do ustawodawstwa i praktyki dopuszczającej stosowanie tajnych środków nadzoru, Trybunał wielokrotnie powtarzał swoje podejście z *Klass i Inni* (zobacz, *inter alia*, *Weber i Saravia* (dec.), nr 54934/00, § 78, ETPCz 2006 XI; *Organizacja dla Europejskiej Integracji i Praw Człowieka i Ekimdzhiev przeciwko Bułgarii*, nr 62540/00, §§ 58 do 60, 28 czerwca 2007; *Iliya Stefanov przeciwko Bułgarii*, nr 65755/01, § 49, 22 maja 2008; *Liberty i Inni przeciwko Zjednoczonemu Królestwu*, nr 58243/00, §§ 56 do 57, 1 lipca 2008; oraz *Iordachi i Inni przeciwko Mołdawii,* nr 25198/02, §§ 30 to 35, 10 luty 2009).

36.  W sprawie *Kennedy przeciwko Zjednoczonemu Królestwu* (nr 26839/05, § 124, 18 maja 2010) Trybunał orzekł, że aby ocenić w danym przypadku, czy dana osoba może powoływać się na ingerencję ze względu na sam fakt istnienia przepisów zezwalających na stosowanie środków nadzoru, Trybunał musi wziąć pod uwagę dostępność wszelkich środków odwoławczych na szczeblu krajowym oraz ryzyko zastosowania wobec niej środków nadzoru. Tam, gdzie nie ma możliwości zakwestionowania rzekomego stosowania środków nadzoru na szczeblu krajowym, nie można uznać za nieuzasadnione powszechne podejrzenie i obawy ogółu społeczeństwa, że dochodzi do nadużycia uprawnień w zakresie nadzoru. W takich przypadkach, nawet jeżeli faktyczne ryzyko nadzoru jest niewielkie, istnieje większa potrzeba kontroli Trybunału.

Ostatnio Trybunał przyjął, w sprawie *Roman Zakharov przeciwko Rosji* ([WI], nr 47143/06, §§ 170-172, 4 grudnia 2015), zharmonizowane podejście bazujące na wyroku w sprawie *Kennedy*, zgodnie z którym, po pierwsze, Trybunał bierze pod uwagę zakres stosowania przepisów zezwalających na stosowanie środków nadzoru poprzez zbadanie, czy skarżący może być nim dotknięty ze względu na przynależność do grupy osób, do których skierowane są zaskarżone przepisy lub ze względu na to, że przepisy te mają bezpośredni wpływ na wszystkich użytkowników usług łączności poprzez wprowadzenie systemu, w którym każdy może zlecić przechwycenie korespondencji; a po drugie, Trybunał bierze pod uwagę dostępność lub środki odwoławcze na szczeblu krajowym i dostosuje zakres kontroli uzależniając ją od efektywności tych środków.

37.  Trybunał zauważył, że obecni skarżący zarzucali ingerencję w ich mir domowy, komunikację i prywatność ze względu na sam fakt istnienia prawa pozwalającego na tajny nadzór i brak odpowiednich zabezpieczeń, przyznając, że ich sytuacja osobista lub zawodowa nie miała charakteru, który normalnie mógłby pociągać za sobą zastosowanie środków nadzoru. Myśleli jednak, że są oni szczególnie narażeni na przechwycenie ich komunikacji w wyniku zatrudnienia w organizacjach obywatelskich krytykujących rząd.

38.  Trybunał zauważył, że przynależność do organizacji obywatelskiej nie mieści się w zakresie przyczyn wymienionych w artykule 7/E ust. 1 lit. a) pkt. (ad) i lit. e) Ustawy o Policji, które zasadniczo dotyczą zagrożeń terrorystycznych i operacji ratowniczych z korzyścią dla obywateli węgierskich znajdujących się w niebezpiecznych sytuacjach za granicą. Niemniej jednak wydaje się, że na mocy tych przepisów komunikowanie się każdej osoby na Węgrzech może zostać przechwycone, jeżeli przechwycenie zostanie uznane za konieczne z jednej z przyczyn wymienionych w ustawie (zob. paragraf 16 powyżej). Trybunał uważa, że nie można wykluczyć, że istnieje ryzyko, iż skarżący mogą zostać poddani takim środkom, jeżeli władze uznają, że może to służyć uprzedzeniu lub zapobiegnięciu zagrożeniom przewidzianym w przepisach prawa - tym bardziej, że ustawa zawiera pojęcie „osób zidentyfikowanych ... jako szereg osób”, które mogą obejmować w istocie każdą osobę.

Trybunał przypomniał również, że Trybunał Konstytucyjny, badając skargę konstytucyjną skarżących co do istoty sprawy, w sposób dorozumiany uznał, że przedmiotowe przepisy wpływają na sytuację skarżących w rozumieniu art. 26 ust. 1 Ustawy o Trybunale Konstytucyjnym (zobacz paragraf 19 powyżej).

W tym momencie należy zauważyć, że są oni pracownikami organizacji strażniczej, której działalność była wcześniej podobna w pewnym sensie do działalności dziennikarzy (zobacz *Társaság a Szabadságjogokért przeciwko Węgrom*, nr 37374/05, § 36, 14 kwietnia 2009). Trybunał uwzględnił sugestię skarżących, że wszelka obawa przed byciem podmiotem nadzoru mogłaby mieć wpływ na takie działania (zobacz, *mutatis mutandis*, *Nagla przeciwko Łotwie*, n 73469/10, § 82, 16 lipca 2013). W każdym razie, niezależnie od tego, czy skarżący należą do grupy docelowej, czy też nie, Trybunał uważa, że przepisy te mają bezpośredni wpływ na wszystkich użytkowników systemów łączności i wszystkie domy.

39.  Ponadto, biorąc pod uwagę fakt, że prawo krajowe nie wydaje się przewidywać możliwości wniesienia skargi do niezależnego organu przez osobę, która zarzuca przechwycenie jej komunikacji, Trybunał uważa, że skarżący mogli powoływać się na to, że padli ofiarą naruszenia ich praw wynikających z Konwencji w rozumieniu art. 34 Konwencji.

40.  W odniesieniu do wyczerpania krajowych środków odwoławczych Trybunał uznał, że skarżący zwrócili uwagę władz krajowych, w niniejszym przypadku Trybunału Konstytucyjnego, na istotę ich skargi, tj. rzekomy brak wystarczających gwarancji w przepisach regulujących „artykuł 7/E (3) nadzór”. Przyjmując do wiadomości zastrzeżenie rządu, zgodnie z którym przedmiotowa skarga konstytucyjna koncentrowała się na kilku zasadniczych kwestiach, Trybunał uważa, że ze względu na charakter problemu, system gwarancji poprzedzających środki, przeważający podczas ich stosowania i wynikający z niego jest złożonym zestawem uzgodnień, który należy poddać ocenie w całości (zobacz *Klass i Inni*, cytowany powyżej, §§ 39 do 60). W związku z tym - zakładając, że postępowanie przed Trybunałem Konstytucyjnym było w tych okolicznościach skutecznym środkiem zaradczym – fakt, że skarga konstytucyjna skarżących nie obejmowała wszystkich możliwych kwestii, lecz uwypukliła kilka, nie może zostać podniesiony przeciwko nim, w celu umożliwienia odrzucenia ich skargi z powodu niewyczerpania krajowych środków odwoławczych, w zakresie, w jakim ich oświadczenia złożone przed Trybunałem mogą być postrzegane jako uzupełnienie oświadczeń złożonych przed Trybunałem Konstytucyjnym. (zobacz, *mutatis mutandis*, *Gustafsson przeciwko Szwecji*, 25 kwietnia 1996, § 51, *Sprawozdania* 1996‑II).

41.  Ponadto Trybunał stwierdził, że skarga ta nie jest w sposób oczywisty nieuzasadniona w rozumieniu art. 35 ust. 3 lit. a) Konwencji. Stwierdził ponadto, że nie jest ona nieuzasadniona z jakichkolwiek innych powodów. Musi zatem zostać uznana za dopuszczalną.

B.  Przedmiot skargi

1.  Stanowiska stron

(a)  Rząd

42.  W odniesieniu do konieczności uzyskania zezwolenia sądowego w kontekście art. 8 Rząd odniósł się do sprawozdania Komisji Weneckiej w sprawie demokratycznego nadzoru nad służbami bezpieczeństwa (CDL-AD (2007)016, przyjętego na 71. sesji plenarnej Komisji Weneckiej w Wenecji w dniach 1-2 czerwca 2007 r.). Opierając się na kilku spostrzeżeniach poczynionych w tym sprawozdaniu, Rząd stwierdził, że sądy krajowe nie były właściwe do określenia konieczności gromadzenia informacji wywiadowczych do celów bezpieczeństwa narodowego ze względu na charakter danych, które mają być oceniane, nieodłączną subiektywność oceny ryzyka, polityczny charakter pojęcia bezpieczeństwa narodowego oraz szeroki margines uznania przyznany Rządowi w tej dziedzinie.

43.  Zdaniem Rządu, nieodłączną cechą orzeczenia sądowego było zbadanie przez sędziego zgodności proponowanej decyzji z zasadami prawa pozytywnego lub zasadami, które można wywnioskować z prawa pozytywnego. W dziedzinie wydawania zezwoleń na gromadzenie informacji wywiadowczych związanych z bezpieczeństwem narodowym nie istniały żadne pozytywne przepisy określające dokładne kryteria dające podstawy do wydania decyzji sądowych. Powodem tego było to, że zezwalając na gromadzenie informacji tajnych dotyczących bezpieczeństwa narodowego, decyzja, za którą decydent ponosi odpowiedzialność polityczną, miała zostać podjęta poprzez ocenę interesów bezpieczeństwa kraju oraz uwzględnienie wewnętrznych i zagranicznych aspektów politycznych. W związku z tym Minister Sprawiedliwości - ponoszący odpowiedzialność polityczną - był osobą bardziej kompetentną niż sędziowie do podejmowania takich decyzji. W każdym razie doświadczenie pokazało, że kontrola sądowa w tej dziedzinie nie była bardziej trafna niż nadzór rządowy.

44.  Ponadto Rząd ponownie podkreślił, że działalność Ministra Sprawiedliwości związana z wydawaniem zezwoleń w zakresie bezpieczeństwa narodowego była zawsze kontrolowana przez parlamentarną komisję ds. bezpieczeństwa narodowego oraz przez rzecznika ochrony danych i nie było oznak wskazujących, że mechanizm zatwierdzania był formalny lub arbitralny.

45.  Wreszcie Rząd twierdził - opierając się na uwagach Trybunału w sprawach *Klass i In*. (cytowany powyżej), *Goranova-Karaeneva przeciwko Bułgarii* (nr 12739/05 z dnia 8 marca 2011 r.) i *Golder przeciwko Zjednoczonemu Królestwu* (21 lutego 1975 r., seria A nr 18) - że skarga dotycząca braku skutecznego środka odwoławczego na mocy art. 13 była w oczywisty sposób niedopuszczalna.

(b)  Skarżący

46.  Odpowiadając na argumenty oparte na sprawozdaniu Komisji Weneckiej, skarżący podkreślili, że ponieważ sądy powszechne w praktyce często napotykały trudności w radzeniu sobie z dużym marginesem uznania przyznanym Rządowi w tej dziedzinie, jak zauważyła Komisja Wenecka, nie można stwierdzić, że kontrola sądowa doprowadziła do mniej właściwej kontroli tajnego nadzoru dla celów bezpieczeństwa narodowego. Rzeczywisty wniosek płynący ze sprawozdania jest taki, że jedynie kompleksowe gwarancje mające na celu zaangażowanie sędziów w kontrolę służb bezpieczeństwa mogą zapewnić odpowiednią ochronę jednostek. Jak wskazano w sprawozdaniu Konwencji Weneckiej, „aby zapewnić skuteczność kontroli sądowej, sędziowie muszą być niezależni i posiadać niezbędną wiedzę fachową”.

47.  Skarżący podkreślili również, że warunki wstępne stosowania specjalnych instrumentów tajnego nadzoru i metod gromadzenia informacji wywiadowczych nie zostały dokładnie określone w ustawie, co może również prowadzić do arbitralnego podejmowania decyzji przy braku kontroli sądowej. W tym względzie skarżący powołali się na orzecznictwo Trybunału, podnosząc, że ograniczenia prawa do prywatności poprzez niejawny nadzór mogą być zgodne z Konwencją jedynie wtedy, gdy ograniczenie to zostało prawidłowo zdefiniowane przez prawo. (cf. *Malone*, cytowany powyżej).

48.  Skarżący twierdzili ponadto, że rzecznik ochrony danych i parlamentarna komisja ds. bezpieczeństwa narodowego nie zastąpiły kontroli sądowej na etapie wydawania zezwoleń, ponieważ stanowią one raczej mechanizmy nadzoru niż środki zaradcze i mają jedynie ogólne konsekwencje niemające wpływu na konkretną sprawę. W odpowiedzi na pytania zadawane tym dwóm organom skarżący twierdziły, że żaden z nich nigdy nie zajmował się sprawą dotyczącą nadzoru nad obywatelami. Potencjalne mechanizmy kontroli nie były zatem skuteczne.

(c)  Strony trzecie

(i)  Center for Democracy and Techonology (CDT)

49.  CDT zwrócił uwagę Trybunału na obecne zaawansowane możliwości Państw w zakresie zaawansowanego i inwazyjnego nadzoru, jak również na ich zdolność do tworzenia szczegółowego profilu działalności i relacji każdej osoby fizycznej z wykorzystaniem przechwyconych danych. Wspomniano w nim o ogromnej ilości informacji, które można pobrać z fizycznie zajętego komputera lub innego osobistego urządzenia elektronicznego. Podkreślono w nim również rozwój możliwości przechwytywania informacji i metadanych, takich jak kontakty i informacje o lokalizacji, poprzez zdalne korzystanie z Internetu lub sieci telefonicznych. Oprócz masowego nadzoru i zaawansowanej analizy przechwyconych danych, Państwa były również w stanie prowadzić ukierunkowany nadzór nad konkretnymi osobami, instalując zdalnie szkodliwe oprogramowanie na urządzeniach, a nawet umożliwiając tajnym służbom nagrywanie naciśnięć klawiszy, dźwięków, zdjęć lub filmów wideo, bez wiedzy właściciela.

50.  Zgodnie z CDT, w świetle takich możliwości nadzorczych art. 8 wymagał nadzoru sądowego nad wszystkimi programami tajnego nadzoru prowadzonymi na potrzeby bezpieczeństwa narodowego. W odniesieniu do tych wyjątkowych przypadków, w których nadzór sądowy był niemożliwy, CDT zwrócił się do Trybunału o udzielenie Układającym się Stronom i skarżącym jasnych wskazówek poprzez przyjęcie zestawu szczegółowych kryteriów służących ustaleniu, czy procedura nadzoru pozasądowego była wystarczająca, aby zapobiec nadużywaniu praw wynikających z art. 8 - chociaż CDT utrzymywał, że art. 8 wymaga jednak kontroli sądowej jako środka ostatecznego. Wreszcie, CDT stwierdził, że każda osoba podlegająca jurysdykcji Układającej się Strony, która ma wiarygodne roszczenie, że padła ofiarą naruszenia art. 8 wynikającego z tajnego krajowego programu nadzoru bezpieczeństwa, musi mieć dostęp do skutecznego środka zaradczego w tym sensie, że organ naprawczy jest zobowiązany do przeprowadzenia dochodzenia w sprawie skargi, a także jest zarówno upoważniony, jak i zobowiązany do zapewnienia skutecznego zadośćuczynienia za naruszenie.

(ii)  Privacy International

51.  Privacy International dokonał przeglądu stosownego orzecznictwa, zarówno Trybunału, jak i sądów krajowych w Europie, Kanadzie i Stanach Zjednoczonych, podkreślając niedawne decyzje potwierdzające, że środki nadzoru, w tym zwykły dostęp do danych zatrzymywanych przez dostawców usług łączności, muszą podlegać kontroli sądowej lub być uzależnione od wydania nakazu sądowego. Ponadto Privacy International zapoznała się z międzynarodowymi standardami praw człowieka dotyczącymi kwestii sądowej kontroli nadzoru, odnosząc się między innymi do ogłoszeń Organizacji Narodów Zjednoczonych oraz Międzynarodowych Zasad Stosowania Praw Człowieka do Nadzoru Łączności, które obejmują potrzebę sądowej kontroli nadzoru oraz potrzebę prawa do skutecznego środka odwoławczego.

2.  Ocena Trybunału

52.  Strony nie pozostają w sporze, co do tego, że środki, do których stosowania TEK jest uprawniony na podstawie art. 56 ustawy o bezpieczeństwie narodowym (zob. pkt. 17 powyżej), to znaczy: przeszukiwanie i prowadzenie nadzoru nad domami skarżących w sposób tajny, sprawdzanie ich poczty i paczek pocztowych, monitorowanie ich komunikacji elektronicznej i transmisji danych komputerowych oraz rejestrowanie wszelkich danych uzyskanych za pomocą tych metod, mogą być rozpatrywane z punktu widzenia pojęć „życia prywatnego”, „domu” i „korespondencji”. Trybunał nie widzi powodu, by twierdzić inaczej (zob. przywołany powyżej § 41 *Klass i in*.).

53.  W samym istnieniu ustawodawstwa, dla wszystkich tych, do których ustawodawstwo mogłoby być stosowane, istnieje zagrożenie nadzoru; zagrożenie to z konieczności uderza w swobodę komunikacji między użytkownikami usług pocztowych i telekomunikacyjnych, a tym samym stanowi „ingerencję władzy publicznej” w wykonywanie przez skarżących prawa do poszanowania życia prywatnego i rodzinnego oraz korespondencji (zob. cytowany powyżej *Klass i in.,* § 41). Biorąc pod uwagę postęp technologiczny, jaki nastąpił od czasu sprawy *Klass i in*., potencjalna ingerencja w pocztę elektroniczną, telefonię komórkową i usługi internetowe, jak również możliwość masowego nadzoru jeszcze bardziej wnikliwie budzi zainteresowanie prawa do ochrony życia prywatnego (zob. *Kopland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, § 41 ETPCz 2007 I).

54.  Jakakolwiek ingerencja może być uzasadniona na mocy art. 8 ust. 2 jedynie wtedy, gdy jest zgodna z prawem, służy realizacji jednego lub większej liczby celów zgodnych z prawem, do których odnosi się art. 8 ust. 2, i jest konieczna w demokratycznym społeczeństwie do osiągnięcia jakiegokolwiek takiego celu. Przepis ten, „ponieważ przewiduje wyjątek od prawa zagwarantowanego przez Konwencję, należy interpretować zawężająco. Uprawnienia do tajnego nadzorowania obywateli, są charakteryzowane jako państwo policyjne, są tolerowane na mocy Konwencji jedynie w takim zakresie, w jakim jest to absolutnie niezbędne dla ochrony instytucji demokratycznych” (zob. *Klass i inni*, cytowane powyżej, § 42).

55.  Trybunał stwierdził, że celem omawianej ingerencji jest ochrona bezpieczeństwa narodowego lub zapobieganie zakłóceniom porządku lub przestępstwom na podstawie art. 8 ust. 2. Nie było to przedmiotem sporu między stronami. Z drugiej strony należy natomiast sprawdzić, czy środki przewidziane w naruszonym prawodawstwie na osiągnięcie wyżej wymienionego celu pozostają pod każdym względem w granicach tego, co jest konieczne w demokratycznym społeczeństwie (patrz *Klass i inni*, cytowany powyżej, § 46).

56.  W swoim orzecznictwie dotyczącym tajnych środków nadzoru Trybunał opracował następujące minimalne zabezpieczenia, które powinny zostać określone prawnie w celu uniknięcia nadużyć władzy: charakter przestępstw, które mogą skutkować nakazem przechwycenia; określenie kategorii osób, którym może być założony podsłuch telefoniczny; ograniczenie czasu trwania podsłuchu telefonicznego; procedura, którą należy stosować przy sprawdzaniu, wykorzystywaniu i przechowywaniu uzyskanych danych; środki ostrożności, jakie należy podjąć przy przekazywaniu danych. (zobacz *Huvig przeciwko Francji*, 24 kwietnia 1990, § 34, Seria A nr 176‑B; *Amann* przeciwko Szwajcarii [WI], nr 27798/95, §§ 56-58, ETPCz 2000‑11; *Valenzuela Contreras przeciwko Hiszpanii*, 30 lipca 1998, § 46, *Sprawozdania* 1998‑V; *Prado Bugallo przeciwko Hiszpanii,* nr 58496/00, § 30, 18 lutego 2003; *Weber i Saravia,* cytowany powyżej, § 95; *Organizacja dla Integracji Europejskiej,* cytowany powyżej, § 76; i *Roman Zakharov*, cytowany powyżej, § 231).

57.  W przypadku równoważenia interesów pozwanego Państwa w zakresie ochrony bezpieczeństwa narodowego poprzez zastosowanie tajnych środków nadzoru z powagą ingerencji w prawo skarżącego do poszanowania jego życia prywatnego, organy krajowe dysponują pewnym marginesem uznania przy wyborze środków służących osiągnięciu uzasadnionego celu ochrony bezpieczeństwa narodowego. Margines ten podlega jednak europejskiemu nadzorowi obejmującemu zarówno prawodawstwo, jak i decyzje dotyczące jego stosowania. Ze względu na ryzyko, że system kontroli ustanowiony w celu ochrony bezpieczeństwa narodowego może pod przykrywką obrony demokracji zagrozić, a nawet zniszczyć demokrację, Trybunał musi być przekonany, że istnieją odpowiednie i skuteczne gwarancje przeciwko nadużyciom. Ocena ta zależy od wszystkich okoliczności sprawy, takich jak charakter, zakres i czas trwania ewentualnych środków, powody, na podstawie których należy na nie zezwolić, organy właściwe do wydawania zezwoleń, przeprowadzania ich i nadzorowania oraz rodzaj środków zaradczych przewidzianych w prawie krajowym. Trybunał musi ustalić, czy procedury nadzoru nad zarządzaniem i wdrażaniem środków ograniczających są takie, że „przeszkadzają” w tym, co jest „niezbędne w demokratycznym społeczeństwie”. (zobacz *Klass i Inni, cytowany powyżej,* §§ 49, 50 i 59; *Weber i Saravia,* cytowany powyżej, §106; *Kvasnica* przeciwko *Słowacji,* nr 72094/01, § 80, 9 czerwca 2009; *Kennedy,* cytowany powyżej, §§ 153 i 154; i *Roman Zakharov*, cytowany powyżej, § 232).

58.  Trybunał stwierdził, że doszło do ingerencji w prawo zagwarantowane przez art. 8 ust. 1 w odniesieniu do ogólnej skargi skarżących dotyczącej zasad „nadzoru na podstawie artykułu 7/E (3)”, a nie w odniesieniu do jakiejkolwiek faktycznej, rzekomo prowadzonej działalności przechwytującej. W związku z tym Trybunał, badając uzasadnienie ingerencji na podstawie art. 8 ust. 2, jest zobowiązany do zbadania samego przepisu oraz wbudowanych w system zabezpieczeń pozwalających na niejawny nadzór, a nie proporcjonalności konkretnych środków podjętych w stosunku do skarżących. W tych okolicznościach zgodność z prawem ingerencji jest ściśle związana z pytaniem, czy spełniono kryterium „konieczności” w odniesieniu do systemu „nadzoru na podstawie artykułu 7/E (3) i w związku z tym właściwe jest, aby Trybunał rozpatrywał wspólnie wymogi „zgodnie z prawem” i „niezbędnością” (zobacz *Kvasnica*, przywołany powyżej, § 84).

59.  Sformułowanie „zgodnie z prawem” z art. 8 ust. 2 wymaga, po pierwsze, aby zaskarżony środek miał jakąś podstawę w prawie krajowym; odnosi się ono również do jakości danego prawa, wymagając, aby było ono zgodne z zasadą państwa prawa i dostępne dla zainteresowanego, który musi ponadto być w stanie przewidzieć jego konsekwencje dla niego (zobacz, między innymi, *Kruslin przeciwko Francji*, 24 kwietnia 1990, § 27, Seria A nr 176-A; *Huvig*, cytowany powyżej, § 26; *Lambert przeciwko Francji,* 24 sierpnia 1998, § 23, *Raporty* 1998-V; *Perry przeciwko Zjednoczonemu Królestwu*, nr 63737/00, § 45, ETPCz 2003-IX (wyciągi); *Dumitru Popescu przeciwko Rumuni (nr 2)*, nr 71525/01, § 61, 26 kwietnia 2007; *Organizacja dla Integracji Europejskiej, cytowany powyżej* § 71; oraz *Liberty*, cytowany powyżej, § 59). „Jakość prawa” w tym sensie oznacza, że prawo krajowe nie tylko musi być dostępne i przewidywalne w jego stosowaniu, ale musi również zapewniać stosowanie środków tajnego nadzoru tylko wtedy, gdy jest to „niezbędne w demokratycznym społeczeństwie”, w szczególności poprzez zapewnienie odpowiednich i skutecznych zabezpieczeń i gwarancji przed nadużyciami (zobacz *Roman Zakharov*, cytowany powyżej, § 236).

60.  Nie kwestionuje się, że przedmiotowa ingerencja miała podstawę prawną. Odpowiednie przepisy zawarte są w ustawach, tj. ustawie o Policji oraz ustawie o bezpieczeństwie narodowym, a ich dostępność nie została zakwestionowana.

61.  Skarżący utrzymywali jednak, że ustawa ta nie jest wystarczająco szczegółowa i precyzyjna, aby spełnić wymóg „przewidywalności” zawarty w art. 8 ust 2, ponieważ nie przewiduje ona wystarczających gwarancji na wypadek nadużyć i arbitralności.

62.  Odniesienie do „przewidywalności” w kontekście przechwytywania komunikacji nie może być takie samo, jak w wielu innych dziedzinach. Przewidywalność w szczególnym kontekście tajnych środków nadzoru, takich jak przechwytywanie komunikacji, nie może oznaczać, że jednostka powinna być w stanie przewidzieć, kiedy władze mogą przechwytywać jej komunikowanie sie, tak aby mogła odpowiednio dostosować swoje postępowanie. Jednak szczególnie w sytuacji, gdy uprawnienia przysługujące władzy wykonawczej są wykonywane w tajemnicy, ryzyko arbitralności jest oczywiste. Konieczne jest zatem wprowadzenie jasnych, szczegółowych zasad przechwytywania rozmów telefonicznych, zwłaszcza że technologia dostępna do ich wykorzystywania jest coraz bardziej zaawansowana. Prawo krajowe musi być wystarczająco jasne, aby dać obywatelom odpowiednie wskazówki co do okoliczności i warunków, w jakich władze publiczne mogą korzystać z takich środków (zobacz *Roman Zakharov*, cytowany powyżej, § 229).

63.  W niniejszej sprawie dwie sytuacje mogą wiązać się z tajnym nadzorem, a mianowicie zapobieganie aktom terrorystycznym na Węgrzech, ich śledzenie i zapobieganie (artykuł 7/E ust. 1 a) ad) Ustawy o Policji) oraz gromadzenie danych wywiadowczych niezbędnych do ratowania obywateli węgierskich, będących w niebezpieczeństwie za granicą (artykuł 7/E ust. 1 e)) (zob. paragraf 16 powyżej). Skarżący skrytykowali te zasady jako niedostatecznie jasne.

64.  Trybunał nie został w pełni przekonany tymi argumentami, przypominając, że brzmienie wielu ustaw nie jest całkowicie precyzyjne, a potrzeba unikania nadmiernej sztywności i dotrzymywania kroku zmieniającym się okolicznościom oznacza, że wiele ustaw jest nieuchronnie tworzonych w sposób, który w mniejszym lub większym stopniu jest niejasny (zobacz *Kokkinakis przeciwko Grecji*, 25 maja 1993, § 40, Seria A nr 260‑A). Trybunał jest usatysfakcjonowany, że nawet w dziedzinie tajnego nadzoru, gdzie przewidywalność budzi szczególny niepokój, zagrożenia związane z aktami terrorystycznymi oraz potrzeby działań ratowniczych są wystarczająco jasne, aby spełniać wymogi legalności. Zdaniem Trybunału wymóg „przewidywalności” prawa nie posuwa się tak daleko, aby zmusić Państwa do przyjęcia przepisów prawnych szczegółowo wymieniających wszystkie sytuacje, które mogą skłonić do podjęcia decyzji o rozpoczęciu tajnego nadzoru. Odniesienie do zagrożeń terrorystycznych lub działań ratowniczych można zasadniczo postrzegać jako dające obywatelom wymagane oznaczenie. (porównaj *Iordachi i Inni*, cytowany powyżej, § 46). Zdaniem Trybunału nic nie wskazuje w tekście właściwego ustawodawstwa, że pojęcie „aktów terrorystycznych”, użyte w art. 7/E ust. 1 lit. a) pkt. ad) Ustawy o Policji, nie odpowiada zbrodni o tej samej nazwie, zawartej w kodeksie karnym (zob. paragraf 16 powyżej).

65.  Jednakże w sprawach dotyczących praw podstawowych byłoby sprzeczne z rządami prawa, jedną z podstawowych zasad demokratycznego społeczeństwa zapisanego w Konwencji, aby swoboda uznania przyznana władzy wykonawczej w dziedzinie bezpieczeństwa narodowego była wyrażana w kategoriach nieograniczonej władzy. W związku z tym ustawa musi jasno określać zakres uprawnień dyskrecjonalnych przyznanych właściwym organom oraz sposób ich wykonywania, mając na uwadze zgodny z prawem cel danego środka, aby zapewnić danej osobie odpowiednią ochronę przed arbitralną ingerencją (zobacz *Roman Zakharov*, cytowany powyżej, § 247).

66.  Trybunał zauważył, że w ramach „artykułu 7/E (3) nadzór” praktycznie każda osoba na Węgrzech może zostać objęta tajnym nadzorem. Ustawodawstwo nie określa kategorii osób, którym w praktyce może zostać odebrana korespondencja. W tym względzie Trybunał zauważył, że warunek dotyczący określenia kategorii osób nachodzi na warunek jasnego zdefiniowania charakteru sytuacji leżących u jego podstaw. Istotne okoliczności, które mogą prowadzić do przechwytywania, omówione w poprzednich paragrafach, stanowią wskazówkę co do kategorii osób, których komunikacja w praktyce zostanie przechwycona. Zgodnie z odpowiednimi przepisami prawa węgierskiego wniosek przedłożony właściwemu ministrowi rządu musi określać, z imienia i nazwiska lub osoby lub grupę osób, mających być podmiotem przechwytywania ich komunikacji i/lub wszelkie inne istotne informacje umożliwiające ich identyfikację, jak również lokal, w odniesieniu do którego ubiega się o zezwolenie (artykuł 57 ust. 2 ustawy o bezpieczeństwie narodowym, zob. paragraf 17 powyżej).

67.  Poważne obawy budzi jednak fakt, że pojęcie “osób zidentyfikowanych .... jako szereg osób” może obejmować rzeczywiście każdą osobę i być interpretowane jako torujące drogę nieograniczonemu nadzorowi dużej liczby obywateli. Trybunał zauważył brak jakichkolwiek wyjaśnień w ustawodawstwie krajowym co do sposobu praktycznego stosowania tego pojęcia (patrz: *mutatis mutandis*, cytowany powyżej *Roman Zakharov*, § 245). W opinii Trybunału kategoria ta jest zbyt szeroka, ponieważ nie ma żadnego rodzaju wymogu, aby władze wykazywały faktyczny lub domniemany związek między osobami lub grupami osób „zainteresowanych” i zapobieganiem wszelkim zagrożeniom terrorystycznym - nie mówiąc już o tym, że w sposób umożliwiający przeprowadzenie przez osobę zezwalającą, analizy która odpowiedziałaby na pytanie bezwzględnej konieczności (zob. pkt. 72 i 73 poniżej) w odniesieniu do zamierzonych celów i zastosowanych środków - chociaż taka analiza wydaje się być uzasadniona w art. 53 ust. 2 ustawy o bezpieczeństwie narodowym, zgodnie z którym „gromadzenie informacji wywiadowczych [może być stosowane wyłącznie] w przypadku, gdy potrzebnej informacji wywiadowczej (...) nie można uzyskać w żaden inny sposób”.

68.  Zdaniem Trybunału naturalną konsekwencją przejawów terroryzmu w dzisiejszych czasach, jest to, że rządy uciekają się do najnowocześniejszych technologii zapobiegania takim atakom, w tym masowego monitorowania komunikacji, która może zawierać oznaki zbliżających się incydentów. Techniki stosowane w takich operacjach monitorujących wykazały w ostatnich latach znaczny postęp i osiągnęły poziom zaawansowania, którego przeciętny obywatel nie jest w stanie sobie wyobrazić (zob. uwagi CDT na ten temat w paragrafach 49-50 powyżej), zwłaszcza gdy zautomatyzowane i systemowe gromadzenie danych jest technicznie możliwe i ciągle rozpowszechnia się. W świetle tych postępów Trybunał musi zbadać, czy rozwojowi metod nadzoru, które skutkują masą gromadzonych danych, towarzyszyło równoczesne tworzenie zabezpieczeń prawnych gwarantujących poszanowanie praw zagwarantowanych przez Konwencję. Dane te często tworzą dalsze informacje na temat warunków, w jakich powstały podstawowe elementy przechwycone przez władze, takie jak czas i miejsce, a także używany sprzęt do tworzenia plików komputerowych, fotografii cyfrowych, komunikatów elektronicznych i tekstowych itp. W istocie zaprzeczyłoby to celowi działań Rządu mających na celu utrzymanie terroryzmu na dystans, co przywróciłoby zaufanie obywateli do zdolności utrzymania bezpieczeństwa publicznego, gdyby zagrożenie terrorystyczne zostało paradoksalnie zastąpione przez dostrzegane zagrożenie nieskrępowaną władzą wykonawczą ingerującą w sferę prywatną obywateli poprzez niekontrolowane, lecz dalekosiężne techniki i prerogatywy nadzoru. W tym kontekście Trybunał odsyła również do uwag Trybunału Sprawiedliwości Unii Europejskiej, a w szczególności specjalnego sprawozdawcy Organizacji Narodów Zjednoczonych, podkreślając znaczenie odpowiedniego ustawodawstwa gwarantującego wystarczające zabezpieczenia w obliczu zwiększonych możliwości technicznych władz w zakresie przechwytywania informacji prywatnych (zob. paragrafy 23 i 24 powyżej).

69.  Trybunał przypomniał, że w sprawie *Kennedy* sporne przepisy nie pozwalały na „masowe rejestrowanie ogromnych ilości komunikatów” (zob. cytowany powyżej *Kennedy*, § 160), co było jednym z elementów pozwalających na niestwierdzenie naruszenia art. 8. Jednakże w niniejszej sprawie Trybunał uznał, że wobec braku szczególnych przepisów w tym zakresie lub odmiennych twierdzeń, nie można wykluczyć, że ogólne przepisy ustawy o bezpieczeństwie narodowym mogą zostać przyjęte w celu umożliwienia tak zwanego strategicznego przechwytywania na dużą skalę, co budzi poważne obawy.

70.  Trybunał pragnie dodać, że możliwość uzyskania przez rządy szczegółowego profilu (zob. uwagi CDT na ten temat w pkt. 49 powyżej) najbardziej intymnych aspektów życia obywateli może prowadzić do szczególnie inwazyjnych ingerencji w życie prywatne. W tym kontekście odsyła się do opinii wyrażonych przez Trybunał Sprawiedliwości Unii Europejskiej i Parlament Europejski (zob. paragrafy 23 i 25 powyżej). Zagrożenie to musi podlegać bardzo ścisłej kontroli zarówno na szczeblu krajowym, jak i w ramach Konwencji. Należy wzmocnić gwarancje wymagane na mocy obowiązującego orzecznictwa Konwencji dotyczącego przechwytywania danych, aby rozwiązać problem takich praktyk nadzorczych. Nie ma jednak uzasadnienia, by w niniejszej sprawie zajmować się tą kwestią, ponieważ węgierski system zabezpieczeń wydaje się nie przestrzegać nawet istniejących zasad.

71.  Ponadto, zgodnie z art. 57 ust. 2 lit. b) we wniosku o udzielenie zezwolenia przez ministra, dyrektor powinien uzasadnić konieczność tajnego gromadzenia informacji wywiadowczych (zob. pkt. 17 powyżej). Trybunał nie ma jednak pewności co do tego, czy możliwa lub gwarantowana jest odpowiednia analiza zamierzonych celów i środków stosowanych do realizacji zadań związanych z bezpieczeństwem narodowym. W rzeczywistości sam wymóg uzasadnienia wniosku przez władze, wskazujący na konieczność tajnego nadzoru, nie wystarcza do przeprowadzenia oceny bezwzględnej konieczności (zob. paragrafy 72 i 73 poniżej). Nie istnieje żadna gwarancja prawna nakładająca na TEK obowiązek sporządzenia materiałów pomocniczych, a w szczególności nie ma wystarczającej podstawy faktycznej do zastosowania tajnych środków gromadzenia informacji wywiadowczych, która umożliwiłaby ocenę konieczności zastosowania proponowanego środka i to na podstawie indywidualnego podejrzenia dotyczącego docelowej osoby (zob. *Roman Zakharov*, cytowany powyżej, §§ 259 i 261). Zdaniem Trybunału jedynie takie informacje pozwoliłyby organowi wydającemu zezwolenia na przeprowadzenie odpowiedniego testu proporcjonalności.

72.  Niezależnie od tego, co wynika z art. 53 ust. 2 ustawy o bezpieczeństwie narodowym, Trybunał przypomniał w tym miejscu, że w sprawie *Klass i in*. orzekł, iż „uprawnienia do tajnej kontroli obywateli... są tolerowane przez Konwencję tylko w takim zakresie, w jakim jest to absolutnie niezbędne dla ochrony instytucji demokratycznych"”(zob. przywołany powyżej *Klass i in*. cytowany powyżej § 42, cytowany w pkt. 54 powyżej). Trzeba przyznać, że wyrażenie „bezwzględnie konieczne” stanowi na pierwszy rzut oka test odmienny od tego przewidzianego w art. 8 ust. 2, czyli „niezbędną w demokratycznym społeczeństwie”

73.  Biorąc jednak pod uwagę szczególny charakter omawianej ingerencji oraz potencjał nowoczesnych technologii nadzoru w zakresie naruszania prywatności obywateli, Trybunał uważa, że wymóg „niezbędności w demokratycznym społeczeństwie" należy interpretować w tym kontekście jako wymóg „bezwzględnej konieczności” w dwóch aspektach. Środek tajnego nadzoru może zostać uznany za zgodny z Konwencją, tylko jeżeli jest bezwzględnie konieczny, jako ogólne rozważenie, dla uzyskania istotnych danych w pojedynczej operacji. Zdaniem Trybunału wszelkie środki tajnego nadzoru, które nie odpowiadają tym kryteriom, mogą być przedmiotem nadużyć ze strony władz dysponujących ogromnymi technologiami. Trybunał zauważa, że zarówno Trybunał Sprawiedliwości Unii Europejskiej, jak i specjalny sprawozdawca Organizacji Narodów Zjednoczonych wymagają od tajnych środków nadzoru, aby były odpowiedzią na bezwzględną konieczność (zob. paragrafy 23 i 24 powyżej) - podejście, które sam popiera. Ponadto, szczególnie w tym kontekście Trybunał odnotowuje brak uprzedniego zezwolenia sądowego na przechwycenie, którego znaczenie zostanie przeanalizowane poniżej w paragrafie 75 i następnych. Zabezpieczenie to posłużyłoby do ograniczenia swobody organów ścigania w interpretacji ogólnych pojęć „zainteresowanych osób zidentyfikowanych .... jako szereg osób” poprzez stosowanie ustalonej wykładni sądowej pojęć lub utrwalonej praktyki w celu sprawdzenia, czy w każdym przypadku istnieją wystarczające powody przechwycenia komunikowania się konkretnej osoby fizycznej (patrz: *mutatis mutandis, Roman Zakharov,* cytowany powyżej, § 249). Tylko w ten sposób potrzeba stosowania środków zabezpieczających stanowi koło zapasowe i może być stosowana jedynie w należycie uzasadnionych przypadkach (zob. cytowany powyżej *Roman Zakharov*, § 266).

74.  Ponadto, w odniesieniu do czasu trwania nadzoru, ustawa o bezpieczeństwie narodowym określa po pierwsze okres, po upływie którego zezwolenie na nadzór wygasa (tzn. po upływie maksymalnie 90 dni, zgodnie z art. 58 ust. 4 ustawy o bezpieczeństwie narodowym) oraz po drugie warunki, na jakich możliwe jest przedłużenie. Okres ważności zezwoleń może zostać przedłużony o kolejne 90 dni, a właściwy minister musi zezwolić na takie przedłużenie na podstawie uzasadnionej prośby właściwych służb (patrz: pkt. 17 powyżej). Artykuł 60 stanowi, że zezwolenie musi zostać uchylone, jeżeli nie jest już konieczne, jeżeli kontynuacja nadzoru nie ma szans na osiągnięcie wyników, jeżeli upłynął jego termin lub jeżeli okaże się stanowić naruszenie prawa z jakiegokolwiek powodu. Trybunał nie może jednak pominąć faktu, że z prawa nie wynika jasno - zwłaszcza wobec braku wykładni sądowej - że takie przedłużenie zezwolenia jest możliwe tylko raz lub wielokrotnie, co stanowi kolejny element, który może być przedmiotem nadużyć.

75.  Główną kwestią wspólną zarówno dla etapu zatwierdzania środków nadzoru, jak i ich stosowania, jest brak nadzoru sądowego. Środki te są zatwierdzane przez ministra właściwego do spraw wymiaru sprawiedliwości na wniosek kierownictwa odpowiednich służb bezpieczeństwa, tj. TEK, który ze swojej strony jest wyspecjalizowanym departamentem taktycznym w ramach sił policyjnych, podlegającym Ministerstwu Spraw Wewnętrznych, posiadającym szerokie uprawnienia do stosowania siły w walce z terroryzmem (zob. art. 1 (2) ust. 15 ustawy o policji, cytowanej w paragrafie 16 powyżej). Zdaniem Trybunału, nadzór ten, będący wyjątkowo politycznym (jak zauważył Trybunał Konstytucyjny, zob. pkt. 105 decyzji cytowanej w pkt. 20 powyżej), ale prowadzony przez Ministra Sprawiedliwości, który wydaje się formalnie niezależny zarówno od TEK, jak i od Ministra Spraw Wewnętrznych - nie jest z natury rzeczy w stanie zapewnić wymaganej oceny bezwzględnej konieczności w odniesieniu do celów i środków, o których mowa. W szczególności, pomimo że od służby bezpieczeństwa wymagane jest, aby w swoich wnioskach do ministra o wydanie zezwolenia, przedstawiły konieczność jako taką tajnego gromadzenia informacji, procedura ta nie gwarantuje przeprowadzenia oceny bezwzględnej konieczności, w szczególności w odniesieniu do liczby osób i właściwych pomieszczeń (zob. art. 57 ust. 2 ustawy o bezpieczeństwie narodowym, o którym mowa w ust. 17 powyżej).

76.  Trybunał odnotowuje argumentację Rządu, zgodnie z którą minister ma lepszą pozycję niż sędzia do zatwierdzania lub nadzorowania środków tajnego nadzoru. Chociaż z operacyjnego punktu widzenia kwestia ta może być dyskusyjna, Trybunał nie jest przekonany o tym, jeżeli chodzi o analizę celów i środków pod względem bezwzględnej konieczności. W każdym razie z twierdzeń stron wynika, że środki nadzoru antyterrorystycznego na Węgrzech nigdy nie podlegały kontroli sądowej, z tego powodu nie można dokonać oceny w sprawie ich zalet lub wad. W związku z tym argument Rządu w tej kwestii, Trybunał uznaje za bezzasadny (patrz: *a contrario, Roman Zakharov*, cytowany powyżej, § 259).

77.  Jeżeli chodzi o organ właściwy do wydawania zezwoleń na sprawowanie nadzoru, zezwolenie na podsłuchiwanie połączeń telefonicznych przez organ pozasądowy może być zgodne z Konwencją (zob. np. cytowany powyżej § 51 *Klass i inni*, § 51; *Weber i Saravia*, cytowane powyżej § 115; oraz *Kenned*y, cytowany powyżej, § 31), pod warunkiem, że organ ten jest wystarczająco niezależny od organu wykonawczego (zob. cytowany powyżej *Roman Zakharov*, § 258). Polityczny charakter procesu autoryzacji i nadzoru zwiększa jednak ryzyko nadużyć. Trybunał przypomina, że praworządność oznacza m. in., że ingerencja władz wykonawczych w prawa jednostki powinna podlegać skutecznej kontroli, która powinna być normalnie zapewniona przez sądownictwo, przynajmniej w ostateczności, poprzez kontrolę sądowniczą dającą najlepsze gwarancje niezależności, bezstronności i odpowiedniego postępowania. W dziedzinie, w której nadużycia są potencjalnie tak łatwe w indywidualnych przypadkach i mogą mieć tak szkodliwe konsekwencje dla społeczeństwa demokratycznego jako całości, zasadniczo pożądane jest powierzenie kontroli nadzorczej sędziemu (zob. *Klass i inni*, cytowany powyżej, §§ 55 i 56). Trybunał przypomniał, że w sprawie *Dumitru Popescu* (cytowany powyżej §§ 70-73) Trybunał wyraził pogląd, że albo organ wydający zezwolenia na przechwytywanie danych powinien być niezależny, albo że działalność organu wydającego zezwolenie powinna być kontrolowana przez sędziego lub niezależny organ. W związku z tym, w tej dziedzinie, regułą powinno być sprawowanie kontroli przez niezależny organ, zazwyczaj sędziego posiadającego szczególną wiedzę fachową (patrz: przywołany powyżej *Klass i inni*, §§ 42 i 55). Zatwierdzenie *ex ante* takiego środka nie jest wymogiem bezwzględnym samo w sobie, ponieważ w przypadku znacznego nadzoru sądowego po fakcie może ono stanowić przeciwwagę dla niedociągnięć w wydawaniu zezwolenia (zob. cytowany powyżej § 167 *Kennedy*). W istocie, pod pewnymi względami i w pewnych okolicznościach Trybunał stwierdził już wcześniej, że konieczne jest uprzednie (*quasi*) wydanie zezwolenia sądowego, na przykład w odniesieniu do tajnych środków nadzoru skierowanych do mediów. W tym względzie Trybunał orzekł, że przegląd *post factum* nie może przywrócić poufności źródeł dziennikarskich po ich zniszczeniu (zob. *Telegraaf Media Nederland Landelijke Media B. V. i in. przeciwko Niderlandom*, nr referencyjny 39315/06, § 101, 22 listopada 2012 r.; w innych okolicznościach konieczne jest uzyskanie zezwolenia *ex ante*, zob. wyrok z dnia 25 marca 1998 r. w sprawie *Kopp przeciwko Szwajcarii*, Zb.1998 II).

W opinii Trybunału nadzór ze strony odpowiedzialnego politycznie członka władzy wykonawczej, takiego jak Minister Sprawiedliwości, nie stanowi wystarczających gwarancji.

78.  Coraz powszechniejsza praktyka Rządów polegająca na przekazywaniu i dzieleniu się między sobą informacjami wywiadowczymi uzyskanymi dzięki tajnemu nadzorowi - praktyka, której przydatność w zwalczaniu międzynarodowego terroryzmu po raz kolejny nie podlega wątpliwości i która dotyczy zarówno wymiany między państwami członkowskimi Rady Europy, jak i innymi jurysdykcjami - jest kolejnym czynnikiem wymagającym szczególnej uwagi, jeżeli chodzi o zewnętrzny nadzór i środki zaradcze.

79.  To właśnie w tym kontekście zewnętrzna, najlepiej sądowa, kontrola *a posteriori* działań związanych z tajnym nadzorem, zarówno w indywidualnych przypadkach, jak i jako nadzór ogólny, zyskuje na znaczeniu (zob. również przywołane powyżej *Klass i in*., §§ 56,70 i 71; *Dumitru Popescu*, cytowany powyżej, § 77; oraz *Kennedy*, cytowany powyżej, §§ 184-191), umacniając zaufanie obywateli, że nawet w tej delikatnej dziedzinie działają gwarancje praworządności i zapewnione jest zadośćuczynienie za wszelkie utrzymujące się nadużycia. Znaczenia tej kontroli nie można przecenić ze względu na wielkość puli informacji, które mogą uzyskać władze stosujące wysoce skuteczne metody i przetwarzające masowo dane, potencjalnie o każdej osobie, jeżeli jest ona w taki czy inny sposób powiązana z podejrzanymi osobami lub obiektami planowanych ataków terrorystycznych. Trybunał odnotowuje brak mechanizmu takiej kontroli na Węgrzech.

80.  Trybunał przyznał, że ze względu na charakter współczesnych zagrożeń terrorystycznych mogą zaistnieć sytuacje nadzwyczajne, w których obowiązkowe stosowanie sądowej autoryzacji nie jest wykonalne, przyniosłoby skutek przeciwny do zamierzonego ze względu na brak specjalistycznej wiedzy lub oznaczałoby po prostu stratę cennego czasu. Odnosi się to szczególnie do obecnych zawirowań spowodowanych atakami terrorystycznymi, do których dochodzi na całym świecie i w Europie, które zbyt często pociągają za sobą poważne ofiary śmiertelne, wiele ofiar i znaczne straty materialne, co nieuchronnie rozpowszechnia poczucie braku bezpieczeństwa wśród obywateli. Spostrzeżenia poczynione w tej kwestii przez Trybunał Sprawiedliwości w sprawie *Klass i in.* są równie ważne w okolicznościach niniejszej sprawy: „społeczeństwa demokratyczne są obecnie zagrożone wysoce wyrafinowanymi formami szpiegostwa i terroryzmu, w związku z czym państwo musi być w stanie, aby skutecznie przeciwdziałać takim zagrożeniom, prowadzić tajną kontrolę nad elementami wywrotowymi w ramach swojej jurysdykcji. Trybunał musi zatem uznać, że istnienie niektórych przepisów przyznających uprawnienia tajnego nadzoru nad mailami, pocztą i telekomunikacją jest w wyjątkowych okolicznościach niezbędne w demokratycznym społeczeństwie, w interesie bezpieczeństwa narodowego i/lub zapobiegania zakłóceniom porządku lub przestępczości” (cytowany powyżej §48).

81.  Ponadto, jeżeli chodzi o szczególnie nagłe sytuacje, ustawa zawiera przepis, zgodnie z którym dyrektor służby może sam zezwolić na stosowanie tajnych środków nadzoru przez okres nieprzekraczający 72 godzin (zob. artykuły 58 i 59 ustawy o bezpieczeństwie narodowym, cytowanej w ust. 17 powyżej). Zdaniem Trybunału to wyjątkowe uprawnienie powinno wystarczyć do rozwiązania wszelkich sytuacji, w których zewnętrzna kontrola sądowa wiązałaby się z ryzykiem utraty cennego czasu. Środki takie muszą być jednak poddane ocenie *post factum*, co jest z reguły wymagane w przypadkach, gdy nadzór został uprzednio zatwierdzony *ex ante* przez organ pozasądowy.

82.  Trybunał odnotowuje w tym punkcie, odpowiedzialność władzy wykonawczej za sporządzenie sprawozdania z takich operacji dla komisji parlamentarnej w sposób ogólny, a nie w odniesieniu do poszczególnych przypadków. Niemniej nie jest w stanie wskazać żadnych przepisów ustawodawstwa węgierskiego, które zezwalałyby na zastosowanie środka zaradczego przyznanego w ramach tej procedury podczas stosowania środków tajnego nadzoru wobec tych, którzy podlegają tajnemu nadzorowi, ale z konieczności są o nich nieświadomi. Minister jest zobowiązany do przedstawienia właściwej komisji parlamentarnej ogólnego sprawozdania, co najmniej dwa razy w roku, na temat funkcjonowania krajowych służb bezpieczeństwa, które nie wydaje się jednak dostępne opinii publicznej i w związku z tym wydaje się, że nie zapewnia odpowiednich zabezpieczeń w zakresie kontroli publicznej (zob. cytowany powyżej *Roman Zakharov*, § 283). Komisja ma prawo z własnej inicjatywy zwrócić się do ministra i dyrektorów służb o informacje na temat działalności służb bezpieczeństwa narodowego. Niemniej, Trybunał nie jest przekonany, że kontrola ta jest w stanie zadośćuczynić wszelkim indywidualnym skargom spowodowanym przez tajny nadzór lub skutecznie kontrolować, co wpływa na same operacje, tj. codzienne funkcjonowanie organów nadzoru, zwłaszcza że nie wydaje się, aby komisja miała szczegółowy dostęp do odpowiednich dokumentów. Zakres ich nadzoru jest zatem ograniczony (zob. *mutatis mutandis*, cytowany powyżej *Roman Zakharov*, § 281).

83.  Ponadto procedura składania skarg opisana w artykule 11 ust. 5 ustawy o bezpieczeństwie narodowym wydaje się mieć niewielkie znaczenie, ponieważ obywatele poddani tajnemu nadzorowi nie zapoznają się z zastosowanymi środkami. W odniesieniu do tej ostatniej kwestii, Trybunał podziela pogląd Komisji Weneckiej, zgodnie z którym „osoby, które twierdzą, że Państwo błędnie postępowało w innych dziedzinach, mają prawo do dochodzenia odszkodowania przed sądami. Skuteczność tego prawa zależy jednak od znajomości przez jednostkę zarzucanego czynu niedozwolonego oraz od możliwości przedstawienia w tym zakresie dowodów do oceny sądu” (zob. paragraf 243 sprawozdania, cytowany w paragrafie 21 powyżej). Skargę złożoną na podstawie art. 11 ust. 5 ustawy o bezpieczeństwie narodowym rozpatruje minister spraw wewnętrznych, który nie wydaje się wystarczająco niezależny (zob. cytowane wyżej *Stowarzyszenie Integracji Europejskiej*, § 87; oraz *Roman Zakharov*, cytowany powyżej, § 278).

84.  Trybunał odnotowuje ponadto, że do dowodów przedstawionych przez skarżących, Komisarz ds. Praw Podstawowych nigdy dotąd nie poddał wątpliwość kwestii tajnego nadzoru (zob. paragraf 18).

85.  W każdym razie Trybunał przypomniał, że w sprawie *Klass i in*. połączenie mechanizmów nadzoru, brak formalnej kontroli sądowej, zostało uznane za dopuszczalne w szczególności ze względu na „wstępną kontrolę przeprowadzoną przez urzędnika posiadającego uprawnienia do pełnienia funkcji sądowniczych” (cytowany powyżej, § 56). Węgierski system wydawania zezwoleń nie przewiduje jednak tego typu urzędnika. Węgierski Komisarz ds. Praw Podstawowych nie wydaje się osobą, która musi sprawować lub sprawowała urząd sądowniczy (zob. cytowany powyżej, *Kennedy*, § 57).

86.  Ponadto Trybunał orzekł ponadto, że kwestia późniejszego powiadamiania o środkach nadzoru jest nierozerwalnie związana ze skutecznością środków zaradczych, a tym samym z istnieniem skutecznych zabezpieczeń przed nadużyciem uprawnień w zakresie nadzoru, ponieważ z zasady nie ma możliwości odwołania się przez daną osobę, chyba że osoba ta zostanie powiadomiona o środkach podjętych bez jej wiedzy, a tym samym będzie w stanie zakwestionować ich uzasadnienie z mocą wsteczną. Gdy tylko po zakończeniu stosowania środka nadzoru powiadomienie może zostać dokonane bez narażania na szwank celu ograniczenia, informacje powinny zostać przekazane zainteresowanym osobom (patrz: *Weber i Saravia*, cytowany powyżej, § 135; *Roman Zakharov*, cytowany powyżej, § 287). W prawie węgierskim nie przewiduje się jednak żadnego rodzaju powiadomienia o środkach. Fakt ten, w połączeniu z brakiem formalnych środków zaradczych w przypadku nadużyć, wskazuje, że prawodawstwo nie zapewnia odpowiednich zabezpieczeń.

87.  Należy dodać, że chociaż Trybunał Konstytucyjny orzekł, iż różne przepisy prawa krajowego odczytywane łącznie odpowiednio zabezpieczają przechowywanie, przetwarzanie i usuwanie danych, to w szczególności zwraca uwagę na znaczenie indywidualnych skarg wnoszonych w tym kontekście (zob. paragraf 138 decyzji, cytowany w paragrafie 20 powyżej). Zdaniem Trybunału to drugie postępowanie jest ciężko wyobrażalne, ponieważ po raz kolejny, co wynika z ustawodawstwa, zainteresowane osoby nie będą powiadamiane o stosowaniu w stosunku do nich tajnego nadzoru.

88.  Wreszcie Trybunał odnotowuje, że to Rząd powinien przedstawić na odpowiednich przykładach praktyczną skuteczność systemu nadzoru (zob. cytowany powyżej *Roman Zakharov*, § 284). W przedmiotowej sprawie, Rząd nie był jednak w stanie tego zrobić.

89.  Podsumowując, Trybunał nie jest przekonany, że przepisy węgierskie, „artykuł 7/E (3) nadzór” zapewnia dostatecznie precyzyjne, skuteczne i kompleksowe zabezpieczenia w zakresie zezwalania, wykonywania i ewentualnego zadośćuczynienia za stosowanie takich środków.

Biorąc pod uwagę, że zakres środków mógłby obejmować praktycznie każdego, że wydawanie zezwolenia jest realizowane wyłącznie w ramach władzy wykonawczej i bez oceny bezwzględnej konieczności, że nowe technologie umożliwiają rządowi łatwe przechwytywanie dużej ilości danych dotyczących nawet osób spoza pierwotnego zakresu działania, a także biorąc pod uwagę brak skutecznych środków zaradczych, nie mówiąc już o środkach sądowych, Trybunał stwierdza, że doszło do naruszenia art. 8 Konwencji.

II.  DOMNIEMANE NARUSZENIE ARTYKUŁU 6 I ARTYKUŁU 13 KONWENCJI, CZYTANYMI ŁĄCZNIE Z ARTYKUŁEM 8 KONWENCJI

90.  Skarżący zarzucali ponadto, że narażenie ich na tajne środki nadzoru bez kontroli sądowej lub środków odwoławczych stanowi naruszenie ich praw wynikających z art. 6 oraz art. 13 w związku z art. 8 Konwencji.

91.  Rząd zakwestionował ten argument.

92.  Trybunał zauważył, że skargi te są powiązane z tymi rozpatrywanymi powyżej i w związku z tym również należy je uznać za dopuszczalne.

93.  Trybunał przypomniał, że art. 13 nie może być interpretowany jako wymagający środków zaradczych przeciwko prawu krajowemu (zob. wyrok w sprawie *Ostrovar przeciwko Mołdawii* nr 35207/03, § 113, 13 września 2005 r.; *Iordachi*, cytowany powyżej, § 56). W tych okolicznościach Trybunał nie stwierdza naruszenia art. 13 Konwencji w związku z art. 8.

94.  Ponadto, biorąc pod uwagę ustalenie odnoszące się do art. 8 (patrz: paragraf 89 powyżej), Trybunał uważa, że nie jest konieczne zbadanie, czy w tym przypadku doszło do naruszenia art. 6 Konwencji.

III.  ZASTOSOWANIE ARTYKUŁU 41 KONWENCJI

95.  Artykuł 41 Konwencji stanowi:

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

A.  Szkoda

96.  Każdy ze skarżących domagał się 10.000 euro (EUR) z tytułu szkody niemajątkowej.

97.  Rząd stwierdził, że żądanie to jest nadmierne.

98.  Trybunał uważa, że w okolicznościach niniejszej sprawy stwierdzenie naruszenia art. 8 stanowi samo w sobie słuszne zadośćuczynienie za poniesioną szkodę niemajątkową.

B.  Koszty i wydatki

99.  Skarżący domagali się również, łącznie, 7.500 EUR z tytułu poniesionych kosztów i wydatków przed Trybunałem Konstytucyjnym i Trybunałem w Strasburgu, co odpowiada, łącznie, 50 godzinom pracy prawnika, według stawki godzinowej w EUR.

100.  Rząd zakwestionował to żądanie.

101.  Zgodnie z orzecznictwem Trybunału, skarżący jest uprawniony do otrzymania zwrotu kosztów i wydatków wówczas, gdy zostały one faktycznie poniesione oraz są uzasadnione co do wysokości. W niniejszej sprawie, w odniesieniu do dokumentów, które Trybunał miał w swoim posiadaniu i powyższych kryteriów, Trybunał uważa za uzasadnione przyznanie sumy 4.000 EUR pokrywające koszty ze wszystkich tytułów.

C.  Odsetki za zwłokę

102.  Trybunał za słuszne uznaje wyznaczenie wysokości odsetek za zwłokę na podstawie marginalnej stopy procentowej Europejskiego Banku Centralnego powiększonej o trzy punkty procentowe

Z TYCH POWODÓW, TRYBUNAŁ, JEDNOMYŚLNIE,

1.  *Uznaje* skargę za dopuszczalną;

2.  *Stwierdza,* że doszło do naruszenia art. 8 Konwencji;

3.  *Stwierdza,* że nie doszło do naruszenia art. 13 czytanego łącznie z art. 8 Konwencji;

4.  *Stwierdza,* że nie ma potrzeby przeanalizowania skargi z punktu widzenia naruszenia art. 6 Konwencji;

5.  *Stwierdza,* że orzeczenie naruszenia samo w sobie jest wystarczającym słusznym zadośćuczynieniem z tytuły szkody niemajątkowej doznanej przez skarżących;

6.  *Stwierdza,*

(a)  że pozwane państwo wypłaci skarżącym, łącznie, w terminie trzech miesięcy od daty, w której niniejszy wyrok stanie się ostateczny, zgodnie z art. 44 ust. 2 Konwencji, 4.000 EUR (cztery tysiące euro), plus wszelkie należne podatki obciążające skarżących, z tytułu poniesionych kosztów i wydatków, przeliczone na walutę pozwanego państwa według kursu obowiązującego w dniu płatności;

(b)  że od upływu wyżej wskazanego terminu trzech miesięcy aż do momentu uregulowania należności, należne będą odsetki zwykłe od określonej powyżej kwoty, naliczone według stopy równej marginalnej stopie procentowej Europejskiego Banku Centralnego obowiązującej w tym okresie, powiększonej o trzy punkty procentowe;

7.  *Oddala* pozostałą część żądań skarżących w przedmiocie słusznego zadośćuczynienia*.*

Sporządzono w języku angielskim i obwieszczono pisemnie w dniu 12 stycznia 2016 r., zgodnie z regułą 77 §§ 2 i 3 Regulaminu Trybunału.

 Fatoş Aracı V. De Gaetano
 Kanclerz Sekcji Przewodniczący

Zgodnie z art. 45 ust. 2 Konwencji i regułą 74 § 2 Regulaminu Trybunału, opinia odrębna sędziego Pinto de Albuquerque została dołączona do wyroku.

V.D.G.
F.A.

ZGODNA OPINIA ODRĘBNA
SĘDZIEGO PINTO DE ALBUQUERQUE

1.  Izba jest jednomyślna w ocenie, że doszło do naruszenia artykułu 8, niemniej ja jestem nieusatysfakcjonowany uzasadnieniem do wyroku - w dwóch kluczowych kwestiach, Izba celowo odchodzi od wyroku Wielkiej Izby wydanego niedawno w sprawie *Roman Zakharov przeciwko Rosji*[[1]](#footnote-1), który określił europejski standard w masowym nadzorze wywiadowczym oraz cele bezpieczeństwa narodowego. Między uzasadnieniem do wyroku Izby i tym wydanym przez Wielką Izbę są dwa konfrontacyjne punkty odnoszące do kryterium konieczności w ustaleniu tajnych działań nadzorczych oraz stopnia podejrzenia o udział w monitorowanych przestępstwach lub działaniach.

2.  Nie mogę zgodzić się z podejściem Izby, z dwóch ważnych powodów: po pierwsze, ponieważ już wcześniej zająłem odrębne stanowisko w tych kwestiach, w opinii odrębnej dołączonej do wyroku w sprawie *Draksas przeciwko Litwie* dotyczącej podsłuchów telefonicznych oraz innego przechwytywania komunikacji jako tajnego nadzoru oraz mechanizmów gromadzenia danych[[2]](#footnote-2), które nie mogą być mylone ze specjalnym technikami śledczymi występującymi w obrębie prawa karnego[[3]](#footnote-3); po drugie, moja opinia w *Draksas* została potwierdzona, w swej istocie, przez Wielką Izbę w wyżej wspomnianym wyroku dotyczącym Rosji. Stąd też nic nie może usprawiedliwić mojego sprzeciwu wobec ustaleń Wielkiej Izby w sprawie *Roman Zakharov*. Z tego też względu, w niniejszej opinii, pragnę dążyć do obrony ustaleń, podjętych przez Wielką Izbę oraz do zdekonstruowania uzasadnienia przedmiotowego wyroku, w tych względach gdzie się ze sobą różnią.

Masowa inwigilacja dla celów bezpieczeństwa narodowego w prawie międzynarodowym

3.  Od momentu ujawnienia praktyk masowej inwigilacji w czerwcu 2013 roku przez byłego pracownika Agencji Bezpieczeństwa Narodowego Stanów Zjednoczonych (US NSA) Pana Edwarda Snowdena, dyskusja w kwestii ochrony prywatności zyskała nowy rozpęd w Stanach Zjednoczonych. W chłodnej precyzyjnej prognozie, sprawozdanie Specjalnego Sprawozdawcy Narodów Zjednoczonych w sprawie promocji i ochrony prawa do wolności wyrażania opinii, Franka La Rue, dnia 17 kwietnia 2013 roku, w którym przeanalizował skutki nadzorowania przez Stany komunikacji w wykonywaniu praw człowieka do prywatności oraz do wolności wyrażania opinii[[4]](#footnote-4). Natychmiast po ujawnieniu przez Snowdena, w dniu 21 czerwca 2013 roku, Specjalny Sprawozdawca Narodów Zjednoczonych w sprawie ochrony i promocji prawa do wolności wyrażania opinii oraz Specjalny Sprawozdawca Środkowoamerykańskiej Komisji Praw Człowieka do spraw wolności wyrażania opinii uważali za konieczne aby podkreślić ciąg międzynarodowych zasad prawnych w tej kwestii i opublikowali „Połączoną deklarację o programach inwigilacji oraz ich wpływ na wolność wyrażania opinii”[[5]](#footnote-5). Dnia 26 września 2013 roku 35 Międzynarodowa Konferencja Ochrony Danych i Wdrażania Prywatności przyjęła “Rezolucję w sprawie ochrony danych i prywatności w prawie międzynarodowym”. Komisarz postanowili wezwać rządy do opowiedzenia się za przyjęciem dodatkowego protokołu do art. 17 Międzynarodowej Pakt Praw Obywatelskich i Politycznych (MPPOiP), które powinny opierać się na standardach opracowanych i zatwierdzonych przez Konferencję Międzynarodową oraz na postanowieniach zawartych w Komentarzu Generalnym nr 16 do Porozumienia.

4.  W dniu 18 grudnia 2013 r. Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych przyjęło rezolucję 68/167 w sprawie „prawa do prywatności w erze cyfrowej”[[6]](#footnote-6), w której wyrażono głębokie zaniepokojenie negatywnym wpływem, jaki na wykonywanie i korzystanie z praw człowieka może mieć nadzór i przechwytywanie komunikatów - w tym nadzór eksterytorialny i przechwytywanie komunikatów, a także gromadzenie danych osobowych, w szczególności na masową skalę - oraz wezwano państwa członkowskie do ustanowienia lub utrzymania istniejących niezależnych systemów gromadzenia danych osobowych.

5.  W szczególności w dniu 26 marca 2014 r. Komitet Praw Człowieka w swoich uwagach końcowych do czwartego sprawozdania Stanów Zjednoczonych Ameryki w ramach ICCPR[[7]](#footnote-7), zalecił, aby w dniu 26 marca 2014 r. Komitet Praw Człowieka zalecił podjęcie środków mających na celu zapewnienie, aby wszelkie przypadki ingerencji w prawo do prywatności były zgodne z zasadami legalności, proporcjonalności i konieczności, bez względu na narodowość lub lokalizację osób fizycznych, których komunikacja podlega bezpośredniemu nadzorowi. Podkreśliła również, że konieczna jest reforma obecnego systemu nadzoru nad działaniami nadzorczymi w celu zapewnienia jego skuteczności, m. in. poprzez zapewnienie udziału sądów w zatwierdzaniu lub monitorowaniu środków nadzoru oraz rozważenie możliwości ustanowienia silnych i niezależnych mandatów nadzorczych w celu zapobiegania nadużyciom.

 6.  Na wniosek Zgromadzenia Ogólnego, Wysoki Komisarz Narodów Zjednoczonych do spraw Praw Człowieka (UNHCHR) przedstawił w dniu 30 czerwca 2014 r. sprawozdanie na temat prawa do prywatności w erze cyfrowej[[8]](#footnote-8). Sprawozdanie dotyczyło ochrony i promowania prawa do prywatności w kontekście nadzoru krajowego i eksterytorialnego oraz przechwytywania przekazów cyfrowych i gromadzenia danych osobowych, w tym na masową skalę. zaniepokojony doniesieniami w mediach, z których wynika, że Narodowa Agencja Bezpieczeństwa Narodowego w Stanach Zjednoczonych Ameryki oraz Centrala Łączności Rządowej w Wielkiej Brytanii opracowały technologie umożliwiające dostęp do szerokiego zakresu globalnego ruchu internetowego, rejestry połączeń w Stanach Zjednoczonych, elektroniczne książki adresowe poszczególnych osób oraz ogromne ilości innych treści cyfrowych, a także że technologie te zostały wdrożone za pośrednictwem ponadnarodowej sieci obejmującej strategiczne relacje wywiadowcze między rządami, kontrolę regulacyjną nad prywatnymi przedsiębiorstwami i umowami handlowymi, podkreśla, że UNHCHR podkreśliła, co następuje Ukierunkowany nadzór nad komunikacją cyfrową może stanowić niezbędny i skuteczny środek dla służb wywiadowczych i organów ścigania, jeżeli jest on prowadzony zgodnie z prawem międzynarodowym i krajowym, ale „nie wystarczy, aby środki te miały na celu odnalezienie określonych igieł w stogu siana; właściwym środkiem jest wpływ tych środków na składowisko siana w stosunku do zagrażających szkód, a mianowicie, czy środki te są konieczne i proporcjonalne”. Obowiązkowe zatrzymywanie danych przez osoby trzecie, w ramach którego rządy wymagają od przedsiębiorstw telefonicznych i dostawców usług internetowych przechowywania metadanych dotyczących komunikacji z klientami i lokalizacji w celu późniejszego dostępu do nich przez organy ścigania i agencje wywiadowcze, nie wydaje się ani konieczne, ani proporcjonalne. Biorąc pod uwagę rozgraniczenie między wymiarem sprawiedliwości w sprawach karnych a ochroną bezpieczeństwa narodowego, wymiana danych między organami ścigania, organami wywiadowczymi i innymi organami państwowymi może grozić naruszeniem prawa do prywatności, ponieważ środki nadzoru, które mogą być konieczne i proporcjonalne do realizacji jednego uzasadnionego celu, mogą nie być zgodne z celami innego. Państwa powinny zatem podjąć kroki w celu zapewnienia istnienia skutecznych i niezależnych systemów i praktyk nadzoru, zwracając przy tym uwagę na prawo ofiar do skutecznego środka odwoławczego.[[9]](#footnote-9).

7.  Ostatnio w dniu 24 marca 2015 r. Rada Praw Człowieka postanowiła powołać na okres trzech lat specjalnego sprawozdawcę ds. prawa do prywatności. [[10]](#footnote-10).

8.  W ramach Rady Europy ujawnienie praktyk w zakresie nadzoru masowego wzbudziło nowe zainteresowanie Konwencją o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r.[[11]](#footnote-11), oraz Protokołem dodatkowym do Konwencji z dnia 8 listopada 2001 r.[[12]](#footnote-12) o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, dotyczącego organów nadzorczych i transgranicznych przepływów danych z dnia 8 listopada 2001 r. jak również zaleceniem Komitetu Ministrów nr R (87)15 w sprawie wykorzystywania danych osobowych w sektorze policyjnym, przyjętym w dniu 17 września 1987 r., zaleceniem nr R (95)4 w sprawie ochrony danych osobowych w dziedzinie usług telekomunikacyjnych, ze szczególnym uwzględnieniem usług telefonicznych, przyjętym w dniu 7 lutego 1995 r. oraz zaleceniem 1402 (1999)1 Zgromadzenia Parlamentarnego (PACE)1 w sprawie kontroli usług bezpieczeństwa wewnętrznego w państwach członkowskich Rady Europy, przyjętym w dniu 26 kwietnia 1995 r.[[13]](#footnote-13). Ponadto zarówno sprawozdanie Komisji Weneckiej w sprawie demokratycznego nadzoru nad służbami bezpieczeństwa, przyjęte w czerwcu 2007 r.[[14]](#footnote-14), oraz zalecenie nr 11 Komisji Europejskiej przeciwko rasizmowi (ECRI) w sprawie zwalczania rasizmu i dyskryminacji rasowej w policji, przyjęte 29 czerwca 2007 r., zyskało nową aktualność. [[15]](#footnote-15).

9.  Niezwłocznie po publikacji akt Snowdena Komitet Ministrów przyjął w dniu 11 czerwca 2013 r. „Deklarację w sprawie zagrożeń dla praw podstawowych wynikających z technologii cyfrowego śledzenia ruchu i innych technologii nadzoru”, a następnie zalecenie PACE (2024)2013[[16]](#footnote-16) oraz rezolucję (1954)2013 w sprawie bezpieczeństwa narodowego i prawa do informacji, przyjęte w dniu 2 października 2013 r.[[17]](#footnote-17), a Komisarz ds. Praw Człowieka w sprawie „praw człowieka narażonych na ryzyko w momencie rozprzestrzeniania się tajnego nadzoru”, z dnia 24 października 2013 r., wydał dokument „Państwo prawa w Internecie i w szeroko pojętym świecie cyfrowym” z dnia 8 grudnia 2014 r.[[18]](#footnote-18).

10.  Ostatnio, w marcu 2015 r. Komisja Wenecka przyjęła „Aktualizację sprawozdania z 2007 r. w sprawie demokratycznego nadzoru nad służbami bezpieczeństwa oraz sprawozdanie w sprawie demokratycznego nadzoru nad sygnałami agencji wywiadowczych”, w którym dokonano rozróżnienia między nadzorem ukierunkowanym (zbiór niejawny rozmów, telekomunikacja i metadane) a „nadzorem strategicznym”, który „niekoniecznie rozpoczyna się od podejrzenia wobec konkretnej osoby lub osób”. Komisja kładzie nacisk na system autoryzacji sądowej uzupełniony jakąś formą dalszej kontroli przestrzegania warunków. Uprawnienie do „łańcucha kontaktowego”, tj. do identyfikacji osób pozostających ze sobą w kontakcie, powinno być ściśle określone: łańcuch kontaktowy metadanych powinien być zwykle możliwy jedynie w przypadku osób podejrzanych o „faktyczne zaangażowanie w szczególnie poważne przestępstwa”, takie jak terroryzm. W odniesieniu do przeszukiwania danych dotyczących treści powinny mieć zastosowanie zaostrzone wymogi dotyczące uzasadnienia i zabezpieczenia proceduralne, takie jak zaangażowanie rzecznika prywatności. Zdaniem Komisji powiadomienie o objęciu jednego podmiotu nadzorem strategicznym nie jest bezwzględnie wymaganym wymogiem art. 8 konwencji. Jeżeli państwo stosuje ogólną procedurę składania skarg do niezależnego organu nadzoru, może to zrekompensować brak zgłoszenia[[19]](#footnote-19).

11.  W dniu 21 kwietnia 2015 r. PACE przyjęła rezolucję nr 2045 (2015) w sprawie masowego nadzoru, w której wezwała państwa członkowskie Rady Europy i państwa będące obserwatorami do dopilnowania, aby ich przepisy krajowe pozwalały na gromadzenie i analizę danych osobowych, w tym metadanych, wyłącznie za zgodą danej osoby lub na podstawie nakazu sądowego wydanego na podstawie uzasadnionego podejrzenia, że cel jest zamieszany w działalność przestępczą.

12.  W maju 2015 r. Komisarz Praw Człowieka Rady Europy opublikował dokument roboczy zatytułowany "Demokratyczny i skuteczny nadzór nad krajowymi służbami bezpieczeństwa", w którym opowiedziano się za rozszerzeniem niezależnego upoważnienia *ex ante* na nieukierunkowane zbiorcze gromadzenie informacji, zbieranie i dostęp do danych dotyczących łączności, w tym danych przechowywanych przez sektor prywatny, oraz za potencjalnym wykorzystaniem sieci komputerowych. Proces zatwierdzania lub ponownego zatwierdzania środków inwazyjnych powinien podlegać kontroli. Państwa muszą zapewnić, aby osoby fizyczne miały również dostęp do instytucji nadzorczej wyposażonej do wydawania prawnie wiążących nakazów.

13.  Reagując na ogólnoświatową debatę w sprawie masowego nadzoru, Unia Europejska (UE) nie mówiła jednym głosem. Pierwsze stanowisko instytucjonalne zajęła Komisja Europejska, publikując komunikaty do Parlamentu Europejskiego i Rady w sprawie funkcjonowania bezpiecznej przystani z perspektywy obywateli i przedsiębiorstw założonych w UE[[20]](#footnote-20), oraz w sprawie „Przywrócenia zaufania do przepływu danych między UE a USA”[[21]](#footnote-21), oba komunikaty z dnia 27 listopada 2013 r. W następstwie wyroku Trybunału Sprawiedliwości w sprawie *Schrems* Komisja wydała w dniu 6 listopada 2015 r. komunikat do Parlamentu Europejskiego i Rady w sprawie przekazywania danych osobowych z UE do Stanów Zjednoczonych Ameryki na mocy dyrektywy 95/46/WE, w którym podkreśliła, że odnowione i solidne ramy przekazywania danych osobowych do Stanów Zjednoczonych pozostają dla Komisji kluczowym priorytetem, ale jednocześnie określiła alternatywne, np. umowne, narzędzia umożliwiające przepływ danych przez przedsiębiorstwa w celu zgodnego z prawem przekazywania danych do państw trzecich.

14. Parlament Europejskie w swojej rezolucja z dnia 12 marca 2014r. z dnia 12 marca 2014r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych [[22]](#footnote-22), zjadliwie potępił szeroko zakrojone i systemowe całościowe gromadzenie danych osobowych niewinnych ludzi, często obejmujące intymne dane osobowe, w sposób „bezkrytyczny i niepodejrzliwy”, wzywając państwa członkowskie UE do dopilnowania, aby ich służby wywiadowcze podlegały parlamentarnemu i sądowniczemu nadzorowi oraz kontroli publicznej, a także przestrzegały zasad legalności, konieczności, proporcjonalności, należytego postępowania, powiadomień użytkownika i przejrzystość. W ramach stosunków między UE a USA Parlament Europejski wyraźnie domagał się, aby Europejczycy otrzymywali skuteczne gwarancje gwarantujące, że stosowanie nadzoru i przetwarzania danych do celów wywiadu zagranicznego jest proporcjonalne, ograniczone jasno określonymi warunkami i związane z uzasadnionymi podejrzeniami oraz prawdopodobną przyczyną działalności terrorystycznej, podkreślając, że cel ten musi podlegać przejrzystemu nadzorowi sądowemu. Rok później rezolucja Parlamentu Europejskiego z dnia 29 października 2015 r. w sprawie działań następczych po rezolucji Parlamentu Europejskiego z dnia 12 marca 2014 r.[[23]](#footnote-23) wezwała Komisję do przygotowania wytycznych dla państw członkowskich w sprawie sposobu dostosowania wszelkich instrumentów gromadzenia danych osobowych w celu zapobiegania przestępstwom kryminalnym, w tym terroryzmowi, wykrywania ich, prowadzenia dochodzeń w ich sprawie i ich ścigania, do wyroków Trybunału Sprawiedliwości w sprawie zatrzymywania danych oraz w sprawie „bezpiecznej przystani”, wskazując w szczególności na ust. 58 i 59 wyroku w sprawie zatrzymywania danych oraz ustępy do Ostrzegła również przed oczywistą spiralą spadkową, w związku z którą podstawowe prawo do prywatności i ochrony danych osobowych występuje wtedy, gdy każda porcja informacji na temat ludzkiego zachowania jest uważana za potencjalnie przydatną w zwalczaniu przyszłych aktów przestępczych, co z konieczności prowadzi do kultury nadzoru masowego, w ramach której każdy obywatel jest traktowany jako potencjalny podejrzany i prowadzi do podważenia spójności i zaufania społecznego.

15.  W rzeczywistości Trybunał luksemburski odegrał istotną rolę w przedefiniowaniu granic tajnego gromadzenia danych do celów bezpieczeństwa narodowego w UE i poza nią. W sprawie *Maximillian Schrems przeciwko Komisarzowi ds. Ochrony Danych*[[24]](#footnote-24), Trybunał Sprawiedliwości Unii Europejskiej orzekł, że decyzja Komisji w sprawie „bezpiecznej przystani” jest nieważna, ponieważ zezwala na przechowywanie w sposób uogólniony wszystkich danych osobowych wszystkich osób, których dane są przekazywane z UE do Stanów Zjednoczonych bez różnicowania, ograniczeń lub wyjątków w świetle zamierzonego celu i bez ustanawiania obiektywnego kryterium w celu określenia ograniczeń dostępu władz publicznych do danych i ich późniejszego wykorzystania. Trybunał dodał, że przepisy umożliwiające organom publicznym dostęp na zasadzie uogólnienia do treści komunikatów elektronicznych należy uznać za naruszające istotę podstawowego prawa do poszanowania życia prywatnego. Trybunał zauważył również, że uregulowanie, które nie przewiduje możliwości skorzystania przez osobę fizyczną ze środków odwoławczych w celu uzyskania dostępu do danych osobowych jej dotyczących lub uzyskania sprostowania lub usunięcia takich danych, narusza istotę podstawowego prawa do skutecznej ochrony sądowej, ponieważ istnienie takiej możliwości jest nieodłącznie związane z istnieniem praworządności. Trybunał uznał wreszcie, że decyzja w sprawie „bezpiecznej przystani” odmawia krajowym organom nadzorującym ochronę danych uprawnień, jeżeli dana osoba kwestionuje zgodność decyzji z ochroną prywatności oraz podstawowymi prawami i wolnościami jednostki. Trybunał orzekł, że Komisja nie jest uprawniona do ograniczania w ten sposób uprawnień krajowych organów nadzoru.

W połączonych sprawach *Digital Rights Ireland* oraz *Seitinger i Inni*[[25]](#footnote-25), Trybunał luksemburski orzekł już nieważność dyrektywy 2006/24/WE w sprawie zatrzymywania danych, która nakłada na dostawców publicznie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązek zatrzymywania wszystkich danych o ruchu i lokalizacji (lub metadanych) przez okresy od sześciu miesięcy do dwóch lat, w celu zapewnienia dostępności danych do celów dochodzenia, wykrywania i ścigania poważnych przestępstw, zgodnie z definicjami zawartymi w prawie krajowym każdego państwa członkowskiego. Zarówno indywidualnie, jak i w ujęciu łącznym, te możliwości nadzoru pozwoliły państwu na stworzenie precyzyjnego obrazu najbardziej intymnych aspektów życia jednostki. Potencjalne zagrożenie dla prywatności wynikające z takiego obowiązkowego, niebudzącego podejrzeń i nieprzeznaczonego na określony cel obowiązku zatrzymywania danych, wywołujące w umysłach zainteresowanych osób poczucie, że ich życie prywatne podlega stałemu nadzorowi, naruszyło art. 7 i 8 Karty praw podstawowych Unii Europejskiej[[26]](#footnote-26).

16.  Wreszcie, europejskie organy ochrony danych przedstawiły swoje poglądy na temat zagrożeń dla prywatności wynikających z zastosowania narzędzi masowego nadzoru. W dniu 20 lutego 2014 r. Europejski Inspektor Ochrony Danych wydał opinię w sprawie komunikatów Komisji do Parlamentu Europejskiego i Rady w sprawie „Odbudowania zaufania do przepływu danych UE-USA” oraz w sprawie „funkcjonowania bezpiecznej przystani z perspektywy obywateli i przedsiębiorstw UE ustanowionych w UE”[[27]](#footnote-27). Następnie grupa robocza art. 29 opublikowała swoją opinię 4/2014 w sprawie nadzoru łączności elektronicznej do celów wywiadu i bezpieczeństwa narodowego, z dnia 10 kwietnia 2014 r[[28]](#footnote-28). W dniu 26 listopada 2014 r. zgromadzenie Europejskich organów ochrony danych zebrane w grupie roboczej art. 29 wydało wspólne oświadczenie. [[29]](#footnote-29).

Zastosowalność standardów prawa międzynarodowego do niniejszej sprawy

Kategorie monitorowanych przestępstw lub działań

17.  Ustawa nr XXXIV z 1994 o Policji (Ustawa o Policji) nie zawiera żadnej definicji „aktu terrorystycznego” lub „działań terrorystycznych”, co ostatecznie mogłoby podnieść problem dotyczący kwestii przewidywalności ram prawnych gromadzenia danych wywiadowczych do celów bezpieczeństwa narodowego, zgodnie z artykułem 7/E (3). Można argumentować, że odniesienie w art. 69 ust. 5 do „aktu terrorystycznego” w rozumieniu art. 261 dawnego kodeksu karnego i art. 314- 316 nowego kodeksu karnego wypełnia lukę pojęciową i w związku z tym pojęcia te odnoszą się do definicji kodeksu karnego, jak stwierdzono w paragrafie 64 wyroku.[[30]](#footnote-30). W związku z tym środek ochronny, o którym mowa w paragrafie 231 w sprawie *Roman Zakharov* („charakter przestępstw, które mogą prowadzić do wydania nakazu przechwycenia”), jest określony w prawie węgierskim z zachowaniem niezbędnego stopnia jasności i precyzji.[[31]](#footnote-31).

**Stopień podejrzenia o udział w monitorowanych przestępstwach lub działaniach**

18.  Ustawa nr CXXXV z 1995 r. o Służbach Bezpieczeństwa Narodowego ("Ustawa o bezpieczeństwie narodowym") nie zawiera żadnego wymogu, aby monitorowane osoby podlegały normie „uzasadnionego podejrzenia”, określonej w paragrafach 260,262 i 263 *Roman Zakharov*, a poprzednio w paragrafie 51 *Iordachi i in.[[32]](#footnote-32).* Tym jedynym standardem ustanowionym przez prawo węgierskie jest standard „zidentyfikowania zainteresowanych osób z imienia lub nazwiska lub grupy osób” (artykuł 57 ust. 2 lit. a) ustawy o bezpieczeństwie narodowym), co w nieunikniony sposób pozwala na nieograniczone uznaniowość ministerialną i „strategiczne przechwytywanie na dużą skalę”[[33]](#footnote-33). W paragrafie 71 niniejszego wyroku Izba wybrała niższy standard „indywidualnego podejrzenia”, co znacznie zmniejsza stopień ochrony określony w wyroku w sprawie *Roman Zakharov*, a wcześniej w sprawie *Iordachi i in*.[[34]](#footnote-34). Co gorsza, przyjęte przez Izbę niemal bezkompromisowe kryterium podejrzenia jest całkowicie sprzeczne z rosnącą troską Organizacji Narodów Zjednoczonych, Rady Europy i Unii Europejskiej o masowy, bezkrytyczny i tajny „nadzór masowy” oraz obecny stan prawa międzynarodowego, jak określono w wyżej wymienionych dokumentach, takich jak rezolucja Zgromadzenia Parlamentarnego 2045 (2015) i jego zalecenie 1402 (1999)1, sprawozdania Komisji Weneckiej z lat 2007 i 2015, Komisji Europejskiej przeciwko rasizmowi ogólne zalecenie polityki nr 11 oraz rezolucjom Parlamentu Europejskiego z dnia 12 marca 2014 r. i 29 października 2015 r.

19.  W argumentacji Izby, jak i Trybunału Konstytucyjnego, ukryte jest założenie, że ochrona bezpieczeństwa narodowego nie ogranicza się do dochodzenia w sprawie przeszłych, trwających lub przyszłych przestępstw i dlatego kryterium „uzasadnionego podejrzenia” powinno być uchylone. Założenie to jest błędne w niniejszej sprawie, w świetle litery artykułu 7/E (3) ustawy o policji, która odnosi się konkretnie do zapobiegania, śledzenia i uchylania prób przeprowadzania aktów terrorystycznych na Węgrzech (podsekcja 1) lit. a) pkt. ad)) oraz do ratowania zagrożonych obywateli węgierskich, którzy znajdują się w niebezpieczeństwie grożącego im i zagrażającego życiu zagrożenia aktem wojny, konfliktu zbrojnego, wzięcia zakładników lub działań terrorystycznych poza terytorium Węgier („Węgry”). Jak wiadomo, zadania te dotyczą albo zapobiegania przestępstwom terrorystycznym na Węgrzech, albo działań ratowniczych w sytuacjach zagrożenia, wojny, konfliktów zbrojnych, wzięcia zakładników lub działań terrorystycznych już trwających poza terytorium Węgier. W obu przypadkach prewencji kryminalnej i akcji ratowniczych nic nie stoi na przeszkodzie stosowaniu kryterium "uzasadnionego podejrzenia", że osoba, której cel ten dotyczy, jest zaangażowana w przyszłe popełnienie aktu terrorystycznego lub w powstanie bezpośredniej sytuacji zagrożenia podczas gromadzenia tajnych danych wywiadowczych przydatnych do wykonywania tych zadań.

20.  Rzeczywistym powodem, dla którego argumentacja Izby nie pozostaje wierna kryterium „uzasadnionego podejrzenia”, jest to, że zakłada ona, iż walka z terroryzmem wymaga "zbioru informacji, które mogłyby zostać pozyskane przez władze stosujące wysoce skuteczne metody i przetwarzające masowo dane, potencjalnie o każdej osobie, gdyby była ona w ten czy inny sposób powiązana z podejrzanymi osobami lub obiektami planowanych ataków terrorystycznych"[[35]](#footnote-35). Niejasność tego języka jest imponująca, zamykając w sobie poszerzający się, uniwersalny i minimalistyczny próg podejrzliwości potrzebny rzekomo do skutecznej walki z terroryzmem. Stwierdzając w ten sposób, Izba lekceważy, że „Trybunał nie uważa, aby istniały podstawy do stosowania różnych zasad dotyczących dostępności i jasności przepisów regulujących z jednej strony przechwytywanie indywidualnych komunikatów, a z drugiej strony bardziej ogólnych programów nadzoru”[[36]](#footnote-36) Ponadto tak optymistyczny język świadczy o iluzorycznym przekonaniu, że globalny nadzór jest *deus ex machina* zdolny do walki z plagą światowego terroryzmu. Co gorsza, tak złośliwy język zaciera fakt, że ożywienie społeczeństwa niesie ze sobą koszmar orwellowski z 1984 roku. W praktyce Izba akceptuje, by posłużyć się słowami Parlamentu Europejskiego, „ustanowienie pełnoprawnego państwa prewencyjnego, zmieniające ustalony paradygmat prawa karnego w społeczeństwach demokratycznych, zgodnie z którym jakakolwiek ingerencja w prawa podstawowe podejrzanych musi zostać zatwierdzona przez sędziego lub prokuratora na podstawie uzasadnionego podejrzenia i musi być uregulowana prawem, promuje w zamian za to połączenia działań organów ścigania i działań wywiadowczych z zatartą i osłabioną ochroną prawną, często niezgodną z demokratyczną równowagą oraz prawami podstawowymi, zwłaszcza domniemaniem niewinności”[[37]](#footnote-37).

Test konieczności

21.  Artykuł 53 ustawy o bezpieczeństwie narodowym przewiduje test konieczności. W paragrafach 67,71,72,74,74,75 i 88 wyroku wykorzystano kryterium "bezwzględnej konieczności" i odesłano do niego do dwóch celów: ochrony instytucji demokratycznych i nabywania istotnej inteligencji w ramach pojedynczej operacji.[[38]](#footnote-38). To twórcze przeredagowanie testu prawnego rodzi szereg problemów. Po pierwsze, jest to kryterium surowsze niż w paragrafach 233 i 236 *Roman Zakharov* [[39]](#footnote-39). Po drugie, nie odpowiada on luźniejszemu kryterium stopnia podejrzenia o udział w monitorowanych przestępstwach lub działaniach. Jest logicznie niespójne, że ten sam wyrok nakłada „kryterium bezwzględnej konieczności” w celu określenia środka nadzoru, ale jednocześnie przyjmuje bardzo luźne kryterium dotyczące stopnia podejrzenia o udział w monitorowanych przestępstwach lub działaniach, jak wykazano powyżej. Logicznie rzecz biorąc, krytykowanie zbyt obszernego tekstu węgierskiej ustawy jest niespójne, gdy odnosi się ona do „osób objętych dochodzeniem zidentyfikowanych jako szereg osób”, a jednocześnie akceptuje nieprecyzyjny pod względem językowym i nieprecyzyjny pod względem prawnym test "indywidualnego podejrzenia", aby uzasadnić zastosowanie środka nadzoru. Po trzecie, Izba nie wyjaśniła w jaki sposób "kryterium bezwzględnej konieczności" polega na tym, że powiązała je jedynie z zamierzonymi celami. W orzeczeniu w żadnym miejscu wyjaśniono, że test konieczności uzasadnia nakazanie każdej operacji nadzoru tylko wtedy, gdy ustalenie faktów przy użyciu innych mniej inwazyjnych metod okazało się nieskuteczne lub, wyjątkowo, jeżeli inne mniej inwazyjne metody uznaje się za mało prawdopodobne do powodzenia[[40]](#footnote-40).

**Wykaz specjalnych technik nadzoru i ich maksymalny czas trwania**

22.  Artykuł 56 ustawy o bezpieczeństwie narodowym zawiera wyczerpujący wykaz specjalnych technik dochodzeniowych, które obejmują przeszukiwanie i nadzór nad lokalami mieszkalnymi, przechwytywanie poczty i łączności elektronicznej oraz przechwytywanie danych komputerowych i sieciowych. Jednakże w artykule 58 nie określono maksymalnego terminu dla środków nadzoru, jak przewidywał paragraf 231 *Roman Zakharov*[[41]](#footnote-41). Przewiduje on jedynie maksymalny termin 90 dni na każdy wniosek, z możliwością nieograniczonego przedłużenia terminu dla Ministra Sprawiedliwości. Ponadto Minister Sprawiedliwości nie ma dostępu do wyników trwającej operacji nadzoru, gdy jest on wzywany do podjęcia decyzji o jej przedłużeniu, co w oczywisty sposób ułatwia zwykłe stemplowanie wniosku o przedłużenie.

**Procedura wydawania zezwoleń i rewizja**

23.  Ustawa o bezpieczeństwie narodowym nie przewiduje upoważnienia niezależnego organu do podejmowania decyzji o rozpoczęciu działań w zakresie nadzoru (etap pierwszy lub rewizja *ex ante*), ponieważ art. 58 odnosi się jedynie do Ministra Sprawiedliwości jako jedynego organu rozpatrującego wniosek o zastosowanie tajnego nadzoru, bez możliwości dalszego odwołania się od tej decyzji[[42]](#footnote-42). Ramy prawne nie obejmują badania akt sprawy ani oceny faktycznych i prawnych podstaw zezwolenia na stosowanie tajnego nadzoru przez niezależny organ, najlepiej sędziego, jak stwierdził paragraf 233 *Roman Zakharov*, podążając w ślad *Klass i in*.[[43]](#footnote-43). W związku z rozszerzonym konsensusem w zakresie prawa międzynarodowego, o którym mowa powyżej, oraz powagą obecnych zagrożeń dla prywatności obywateli, praworządności i demokracji nadszedł czas, aby nie rezygnować z podstawowej gwarancji autoryzacji sądów i kontroli sądowej w zakresie niejawnego nadzoru nad gromadzeniem informacji[[44]](#footnote-44). Gwarancja sądowa nie jest oczywiście sprzeczna z dodatkową gwarancją zewnętrzną o charakterze politycznym, np. parlamentarnym.

24.  W omawianym przypadku zewnętrzna kontrola sprawowana przez parlamentarną komisję bezpieczeństwa narodowego i Komisarza ds. Praw Podstawowych nie gwarantuje niezależnej oceny wykonywania uprawnień decyzyjnych przez ministerstwo, zważywszy na brak uprawnień kontrolnych zewnętrznych jednostek nadzorujących w konkretnych przypadkach[[45]](#footnote-45). Ponadto w trakcie dochodzenia dotyczącego krajowych służb bezpieczeństwa Komisarz ds. Praw Podstawowych pozbawiony jest prawie wszystkich istotnych dokumentów, ponieważ nie może on kontrolować rejestrów służących identyfikacji osób współpracujących ze służbami bezpieczeństwa narodowego, dokumentów zawierających dane techniczne dotyczące urządzeń i metod wykorzystywanych przez krajowe służby bezpieczeństwa do gromadzenia informacji wywiadowczych lub dokumentów umożliwiających identyfikację osób korzystających z nich, dokumentów związanych z działaniami szyfrującymi, dokumentów dotyczących bezpieczeństwa instalacji oraz dokumentów związanych z zabezpieczeniami i instalacją, dokumentów, w odniesieniu, do których dostęp umożliwiłby identyfikację źródła informacji lub dokumentów, w odniesieniu do których dostęp naruszałby zobowiązania podjęte przez krajowe służby bezpieczeństwa wobec zagranicznych służb partnerskich [[46]](#footnote-46).

25.  Niedociągnięcia w zewnętrznej kontroli politycznej są słusznie krytykowane przez Izbę, ale uzasadnienie wyroku pomija całościową ocenę późniejszej procedury przeglądu nadzoru, która jest niezbędna do oceny, czy ogólna uczciwość systemu wprowadzonego przez ustawodawcę węgierskiego rekompensuje braki w pierwszym etapie procedury tajnego gromadzenia informacji wywiadowczych[[47]](#footnote-47).

26.  Ustawa o bezpieczeństwie narodowym nie ustanawia niezależnego (tj. sądowego) organu monitorującego i kontrolującego - w oczekiwaniu na operację nadzoru (drugi etap lub etap realizacji) - kwestie takie jak to, czy tajne służby faktycznie stosują się do decyzji zezwalającej na stosowanie tajnych środków operacyjnych, czy wiernie odtwarzają w rejestrach oryginalne dane uzyskane w trakcie operacji oraz czy nadzór jest nadal niezbędny do wykonywania zadań określonych w ustawie, jak podkreślano w paragrafie 251 *Roman Zakharov*[[48]](#footnote-48).

27.  Ponadto, gdy operacja nadzoru zakończy się (trzeci etap lub ocena *ex post*), nie przewiduje się możliwości zapoznania niezależnego (tj. sądowego) organu z wynikami nadzoru, a prawo nie zobowiązuje tego organu do sprawdzenia, czy wymogi prawa zostały spełnione. Nie istnieją żadne przepisy określające z odpowiednią precyzją sposób sprawdzania oryginalnych danych uzyskanych w wyniku nadzoru, procedury zachowania ich integralności i poufności oraz procedurę ich niszczenia[[49]](#footnote-49). Nie ma również niezależnej kontroli tego, czy pierwotne dane są faktycznie niszczone w określonym terminie, jeżeli nadzór okazał się bezowocny. [[50]](#footnote-50).

Procedura w trybie pilnym

28.  Decyzja o trybie pilnym może zostać podjęta przez niezależny organ, taki jak dyrektor krajowych tajnych służb, jedynie w przypadku gdy zwykła procedura spowodowałaby opóźnienie, które pozbawiłoby operację sensu. Artykuł 59 ustawy o bezpieczeństwie narodowym odnosi się do sytuacji, w której „zewnętrzna procedura autoryzacji pociąga za sobą takie opóźnienie, że w danych okolicznościach ewidentnie przeciwdziała interesom skutecznego funkcjonowania Krajowej Służby Bezpieczeństwa”.. Nie ogranicza ona jednak stosowania trybu pilnego do przypadków bezpośrednio zagrażających bezpieczeństwu narodowemu. Ponadto nie stanowi on również, że decyzja dyrektora nie może zostać potwierdzona w krótkim czasie przez niezależny (tj. sądowy) organ posiadający pełne uprawnienia odwoławcze, zgodnie z tym, co zostało określone w paragrafie 266 *Roman Zakharov* oraz wcześniej w paragrafie 16 *Stowarzyszenie dla Integracji Europejskiej i Praw Człowieka oraz Ekimzhiev*[[51]](#footnote-51), ponieważ decyzja dyrektora może zostać potwierdzona lub nie przez Ministra Sprawiedliwości jedynie w ciągu 72 godzin.

**Zakomunikowanie uzyskanych danych osobom trzecim**

29.  Ustawa o bezpieczeństwie narodowym nie określa warunków, które należy spełnić, ani środków ostrożności, jakie należy podjąć w przypadku przekazywania przez służby bezpieczeństwa narodowego uzyskanych danych stronom trzecim, co w szczególności jest wymagane w *Roman Zakharov* w paragrafie 231[[52]](#footnote-52). Niejasne odniesienie w art. 45 do przekazywania danych osobowych "zagranicznym organom przetwarzającym dane w ramach przepisów o ochronie danych osobowych" jest oczywiście niewystarczające.

Obowiązek poinformowania osoby objętej nadzorem

30.  Ustawa o bezpieczeństwie narodowym nie ustanawia obowiązku powiadamiania osoby podlegającej nadzorowi o środkach podjętych po ich zakończeniu, pod warunkiem że interesy bezpieczeństwa narodowego nie są zagrożone przez takie ujawnienie, jak przewiduje paragraf 234 *Roman Zakharov,* również tutaj za *Klass i in*.[[53]](#footnote-53). W węgierskim systemie prawnym nie ma również żadnych szczególnych gwarancji w odniesieniu do tajności informacji zawartych w węgierskim systemie prawnym dotyczących prawnika-pacjenta, lekarza-pacjenta, kapłana-penitenta i dziennikarza [[54]](#footnote-54).

**Brak skutecznych środków zaradczych**

31.  Art. 58 ustawy o bezpieczeństwie narodowym zakazuje odwołań od decyzji Ministra Sprawiedliwości w sprawie wniosku o niejawny środek nadzoru na podstawie art. 7/E ust. 3 ustawy o policji. Brak zgłoszenia *ex post* pogarsza sytuację bezradności osób monitorowanych. W związku z tym procedura składania skarg opisana w sekcjach 11 ust. 5 i 14 ust. 4 lit. c)-f) ustawy o bezpieczeństwie narodowym przewiduje jedynie wirtualną możliwość obrony dla monitorowanych osób[[55]](#footnote-55). W związku z tym osoby znajdujące się pod nadzorem na Węgrzech, podobnie jak w Rosji, nie mają realnych możliwości składania skarg, wniosków lub odwołań od konkretnych nakazów nadzoru, którym zostały poddane[[56]](#footnote-56).

32.  W mało prawdopodobnym przypadku, gdy dana osoba dowie się o środku nadzoru wydanym w odniesieniu do niej, na przykład w przypadku gdy otrzyma przeciek informacji potwierdzających środek, krajowe postępowanie w sprawie skargi nie zapewnia niezależnej i skutecznej oceny przedłożonych skarg. Oprócz tego, co już zostało powiedziane na temat braku uprawnień decyzyjnych parlamentarnej Komisji Bezpieczeństwa Narodowego, należy dodać, że postępowania dotyczące skarg związanych z działalnością służb bezpieczeństwa narodowego są początkowo prowadzone przez Ministra Spraw Wewnętrznych, który ma obowiązek poinformować skarżących o wynikach dochodzenia i podjętych środkach w terminie 30 dni. Minister najwyraźniej nie jest niezależnym organem. Jeżeli skarżący nie jest usatysfakcjonowany, może odwołać się do Komitetu, który może przeprowadzić dochodzenie, jeżeli „waga skargi, zgodnie z jedną trzecią głosów członków komisji, uzasadnia dochodzenie”. Polityczny charakter decyzji komitetu wzmacnia dyskrecjonalna ocena „wagi skargi” i większości głosów oddanych w celu wszczęcia dochodzenia. Komitet może przeprowadzić dochodzenie rozpoznawcze, w trakcie którego może mieć dostęp do odpowiednich dokumentów przechowywanych w rejestrze krajowych służb bezpieczeństwa i przesłuchać pracowników krajowych służb bezpieczeństwa. Jeżeli Komisja uzna, że działalność służb bezpieczeństwa narodowego jest niezgodna z prawem lub w jakikolwiek sposób sprzeczna z ich przeznaczeniem, może jedynie zwrócić się do ministra o podjęcie niezbędnych środków. W związku z tym organ naprawczy nie jest zobowiązany ani do prowadzenia dochodzenia, ani do wnoszenia skutecznych środków odwoławczych, nie mówiąc już o nakazaniu zaprzestania wszelkich trwających nadużyć w nadzorze i niszczenia niezgodnych z prawem danych osobowych. Ostatecznie to minister decyduje, jakie działania, jeśli w ogóle, chce podjąć w odpowiedzi na skargi skarżącego.

33. Ponadto, mimo że art. 50 ust. 2 lit. b) ustawy o bezpieczeństwie narodowym mówi o możliwości usunięcia danych osobowych „nakazanym przez sąd w postępowaniu o ochronę danych”, a art. 48 dopuszcza możliwość „złożenia przez zainteresowane osoby wniosku o usunięcie ich danych osobowych”[[57]](#footnote-57), nie jest jasne, w jaki sposób osoba podlegająca monitorowaniu może żądać usunięcia swoich danych osobowych, jeżeli nie ma nawet możliwości uzyskania informacji o gromadzeniu tych danych osobowych przez osobę podlegającą monitorowaniu.

34.  Podsumowując, poprzez pozbawienie podmiotu będącego przedmiotem tajnego nadzoru jakiegokolwiek powiadomienia o jego istnieniu, a tym samym skutecznej możliwości odwołania się do niego z mocą wsteczną, węgierskie prawo nie przewiduje najważniejszego zabezpieczenia przed niewłaściwym zastosowaniem tajnych środków nadzoru[[58]](#footnote-58). Gdyby Samuel Warren i Louis Brandeis zmierzyli się z tym prawem, bez wątpienia powtórzyliby słowa, które przywołują dla siebie prawo do prywatności: "Intensywność i złożoność życia, troska o postęp cywilizacyjny, sprawiły, że konieczne stało się pewne odosobnienie od świata, a człowiek, pod wyrafinowanym wpływem kultury, stał się bardziej wrażliwy na rozgłos, tak aby samotność i prywatność stały się dla jednostki ważniejsze”[[59]](#footnote-59).

Konkluzja

35.  Dla zasady chciałbym powtórzyć, że system tajnej inwigilacji zaprojektowany w celu ochrony bezpieczeństwa narodowego pociąga za sobą ryzyko osłabienia lub nawet zniszczenia demokracji na gruncie jej obrony”[[60]](#footnote-60). Mając to na uwadze, Izba całkiem słusznie nie osłabiła krytyki Węgierskich ram prawnych dotyczących tajnej i masowej inwigilacji w celu uczynienia bardziej skłonnym do przyjęcia dla Pozwanego rządu. Mimo, że krytyka była słuszna, co do istoty orzeczenia grozi, że nie usunie ono całkowicie poważnych zagrożeń dla prywatności obywateli, praworządności i demokracji wynikających z takich ram prawnych [[61]](#footnote-61). Co gorsza, wybory dokonane przez Izbę wprowadzają do orzecznictwa Trybunału zdecydowaną sprzeczność. Paragraf 71 wyroku wyraźnie odbiega od paragrafów 260,262 i 263 wyroku *Roman Zakharov* i paragrafu 51 wyroku w sprawie *Iordachi i in. przeciwko Mołdawii*, ponieważ Izba posługuje się niejednoznacznym, anodowym, niekwalifikowanym „indywidualnym podejrzeniem” do zastosowania tajnego środka gromadzenia informacji wywiadowczych, natomiast wielka izba posługuje się precyzyjnym, wymagającym i kwalifikowanym kryterium „uzasadnionego podejrzenia”. W połączeniu z wszechobecnym kryterium Izby osłabia się uprawnienia i kontrolę sądowniczą, ponieważ wszelkie „podejrzenia” wystarczą, aby zainicjować ciężką artylerię masowej kontroli państwa nad obywatelami, co wiąże się z oczywistym ryzykiem, że sędzia stanie się jedynie gumowym stemplem rządowej strategii kontroli społecznej Wszechobecne „indywidualne podejrzenie” jest równoznaczne z ogólnym podejrzeniem, tj. z nieistotnością testu podejrzanego w ogóle. W praktyce Izba akceptuje dobrowolnie powszechny, nieuzasadniony (uzasadniony) „nadzór strategiczny”, oparty na podejrzeniach i oparty na faktach, w celu zapewnienia bezpieczeństwa narodowego, mimo jednoznacznego upomnienia, że ta metoda tajnego gromadzenia informacji wywiadowczych dla celów „bezpieczeństwa narodowego, wojskowego, gospodarczego i ekologicznego” została przyjęta przez Wielką Izbę w *Roman Zakharov*. Jedynie interwencja Wielkiej Izby naprawi sytuację.

1. *Roman Zakharov przeciwko Rosji* [WI], nr 47143/06, 4 grudnia 2015. [↑](#footnote-ref-1)
2. *Draksas przeciwko Litwie*, nr 36662/04, 31 lipca 2012. [↑](#footnote-ref-2)
3. Zobacz: moja opinia dołączona do sprawy *Lagutin i Inni przeciwko Rosji,* nr 6228/09, 19123/09, 19678/07, 52340/08 i 7451/09, 24 kwietnia 2014. Sprawa ta jest związana z egzekwowaniem prawa oraz śledztwami w sprawach karnych, których standard różnią się od tajnej inwigilacji dla celów bezpieczeństwa narodowego. Należy odnotować, że Izba często myli te standardy (zobacz, na przykład, paragrafy 22 i 56 wyroku, cytując elementy prawa międzynarodowego i orzecznictwa Trybunału istotnego dla celów śledztw w sprawach karnych). [↑](#footnote-ref-3)
4. A/HRC/23/40. Sprawozdawca opowiedział się za nadzorem sądowym nad Państwem w kwestii inwigilacji komunikacji, za prawem osoby podlegającej monitorowaniu do powiadomienia po zakończeniu operacji oraz prawem do dochodzenia zadośćuczynienia (para. 81 i 82). Przed tym sprawozdaniem specjalny sprawozdawca ONZ ds. propagowania i ochrony praw człowieka i podstawowych wolności w walce z terroryzmem, w dniu 17 maja 2010 r. (A/HRC/14/46) przedstawił “Zestawienie dobrych praktyk w zakresie ram prawnych i instytucjonalnych oraz środków zapewniających poszanowanie praw człowieka przez agencje wywiadowcze w walce z terroryzmem, w tym pod ich nadzorem" (A/HRC/14/46). Na ten temat opublikowano również ważne dokumenty społeczeństwa obywatelskiego. Międzynarodowe zasady dotyczące stosowania praw człowieka w nadzorze”, zatwierdzone przez prawie 400 organizacji pozarządowych i organizacji praw człowieka, zostały wprowadzone w maju 2014 r. Inicjatywa na rzecz Otwartego Społeczeństwa opublikowała w dniu 12 czerwca 2013 r.”Globalne zasady bezpieczeństwa narodowego i prawa do informacji (zasady Tshwane), opracowane przez 22 organizacje i ośrodki akademickie zgodnie z “Zasadami Johannesburga dotyczącymi bezpieczeństwa narodowego, wolności wypowiedzi i dostępu do informacji” przyjętymi przez grupę ekspertów powołaną na mocy art. 19 w 1995 r. oraz “Zasadami nadzoru i odpowiedzialności za służby bezpieczeństwa w demokratyzacji konstytucyjnej” opracowanymi w 1997 r. przez Centrum Studiów Bezpieczeństwa Narodowego i Helsińską Fundację Praw Człowieka w Polsce. [↑](#footnote-ref-4)
5. W paragrafie 9 wspólnej deklaracji stwierdzono, że prawo musi jasno określać kryteria, które należy stosować w celu określenia przypadków, w których nadzór ten jest uzasadniony z punktu widzenia bezpieczeństwa narodowego, oraz że środki takie są dozwolone jedynie w przypadku wyraźnego zagrożenia interesów chronionych oraz gdy szkody, które mogą wynikać, byłyby większe niż interes ogólny społeczeństwa w zachowaniu prawa do prywatności oraz swobodnego przepływu pomysłów i informacji. W każdym razie zbieranie tych informacji ma być monitorowane przez niezależny organ nadzoru, a jego gromadzenie powinno podlegać odpowiednim gwarancjom należytego procesu i nadzorowi sądowemu, w granicach dopuszczalnych w demokratycznym społeczeństwie. [↑](#footnote-ref-5)
6. A/RES/68/167. Rezolucja, współfinansowana przez 57 Państw członkowskich, został powzięta bez głosowania. [↑](#footnote-ref-6)
7. Komisja Praw Człowieka, Konkluzje obserwacji dotyczących czwartego raportu USA, CCPR/C/USA/CO/4,26 marca 2014 r., paragraf 22 lit. d). [↑](#footnote-ref-7)
8. A/HRC/27/37. [↑](#footnote-ref-8)
9. Paragrafy 24-27 i 50 sprawozdania. [↑](#footnote-ref-9)
10. A/HRC/28/L.27. [↑](#footnote-ref-10)
11. ETS nr 108. [↑](#footnote-ref-11)
12. ETS nr 181. [↑](#footnote-ref-12)
13. PACE wyraźnie opowiedziała się za szeroko zakrojoną *a priori* i *ex post facto* kontrolą sądową działań nadzorczych o dużym potencjale naruszania praw człowieka, na podstawie "prawdopodobnej przyczyny przekonania, że dana osoba popełnia, popełniła lub wkrótce popełni przestępstwo" lub "prawdopodobnej przyczyny przekonania, że konkretne komunikaty lub konkretne dowody dotyczące tego przestępstwa zostaną uzyskane w drodze proponowanego przechwycenia lub przeszukania domu, lub że (w przypadku aresztowania) przestępstwo zostanie popełnione". Po zakończeniu obserwacji lub podsłuchu, osoba zainteresowana powinna zostać poinformowana o podjętym środku.. [↑](#footnote-ref-13)
14. CDL-AD(2007)016-e. Komisja Wenecka opowiedziała się za zezwoleniem sądowym i przeglądem działań nadzorczych skierowanych do "indywidualnych przypadków", ale jednocześnie zauważyła, że wiele działań nadzorczych nie jest ukierunkowanych na procedury prawne przedprocesowe, takie jak eksploracja danych, a ten rodzaj działań nadzorczych zazwyczaj nie podlega kontroli sądowej (paragrafy 29,202-204). Ponadto Trybunał przyznał, że “może nie być zbyt wiele konkretnych podejrzeń co do tego, że mogą się one utrzymywać w czasie, gdy wnioskuje się o nadzór, ale inne środki uzyskiwania informacji można uznać za niewykonalne” (paragraf 207). [↑](#footnote-ref-14)
15. CRI(2007)39. ECRI wezwał rządy do wprowadzenia rozsądnego standardu podejrzenia, zgodnie z którym uprawnienia w zakresie kontroli, nadzoru i dochodzeń mogą być wykonywane jedynie w oparciu o obiektywne kryteria. [↑](#footnote-ref-15)
16. Zalecenie zachęcało państwa członkowskie Rady Europy do uwzględnienia zasad Tshwane. [↑](#footnote-ref-16)
17. Uchwała potwierdziła, że neutralność Internetu wymaga, aby władze publiczne, dostawcy usług internetowych i inne podmioty powstrzymały się od stosowania inwazyjnych technologii podsłuchowych, takich jak np. dogłębna kontrola pakietów lub innego rodzaju ingerencja w ruch użytkowników Internetu. [↑](#footnote-ref-17)
18. CommDH/IssuePaper(2014)1. Komisarz stwierdził, że "masowe zatrzymywanie danych dotyczących łączności bez podejrzeń" jest zasadniczo sprzeczne z zasadami praworządności, niezgodne z podstawowymi zasadami ochrony danych i nieskuteczne. Państwa członkowskie nie powinny odwoływać się do niego ani nakładać obowiązku zatrzymywania danych przez osoby trzecie. [↑](#footnote-ref-18)
19. CDL-AD(2015)006, paragrafy 3, 16, 24, 51 oraz 103-105. [↑](#footnote-ref-19)
20. COM(2013) 847 ostateczna. Komisja stwierdziła szereg niedociągnięć i sformułowała 13 zaleceń. Na podstawie tych zaleceń Komisja prowadzi rozmowy z władzami USA od stycznia 2014 r. w celu wprowadzenia odnowionego i wzmocnionego porozumienia w sprawie transatlantyckiej wymiany danych.. [↑](#footnote-ref-20)
21. COM(2013) 846 ostateczna. [↑](#footnote-ref-21)
22. 20013/20188(INI). Niniejsza rezolucja została poprzedzona ważnym „Sprawozdaniem w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych” (A7-0139/2014), z 21 lutego 2014. [↑](#footnote-ref-22)
23. 2015/2635(RSP). [↑](#footnote-ref-23)
24. Sprawa C-362/14, wyrok z dnia 6 października 2015. [↑](#footnote-ref-24)
25. Sprawy C-293/12 i C-594/12, wyrok z dnia 8 kwietnia 2014. [↑](#footnote-ref-25)
26. Trybunał w Luxemburgu niewątpliwie zainspirował się standardami ustanowionymi w dyrektywie w sprawie przechowywania danych w Niemczech w 2010 (BVerfG 125, 260). [↑](#footnote-ref-26)
27. 2014/C 116/04. [↑](#footnote-ref-27)
28. 819/14/EN. Koncentrując się na dostępie do metadanych, grupa robocza stwierdziła, że tajne, masowe i bezkrytyczne programy nadzoru są niezgodne z podstawowymi przepisami UE i nie mogą być uzasadnione walką z terroryzmem ani innymi ważnymi zagrożeniami dla bezpieczeństwa narodowego. Między innymi grupa robocza wezwała do ustanowienia skutecznego, solidnego i niezależnego zewnętrznego nadzoru sprawowanego przez wyznaczony organ przy udziale organów ochrony danych lub przez sam organ ochrony danych. Zalecenia zawarte w opinii oparto na analizie prawnej opublikowanej w dokumencie roboczym z dnia 5 grudnia 2014 r. w sprawie nadzoru łączności elektronicznej na potrzeby wywiadu i bezpieczeństwa narodowego. [↑](#footnote-ref-28)
29. 14/EN WP227. [↑](#footnote-ref-29)
30. Paragraf 64 wyroku [↑](#footnote-ref-30)
31. Zobacz również moją opinię w *Draksas*, cytowany powyżej, strona 26, punkt (2). Nie mogę zatem zgodzić się ze stwierdzeniem Izby, że "wymóg" przewidywalności "prawa nie wykracza aż tak daleko, aby zmusić państwa do uchwalenia przepisów prawnych szczegółowo wymieniających wszystkie sytuacje, które mogą skłonić do podjęcia decyzji o podjęciu działań w zakresie tajnego nadzoru" (paragraf 64 wyroku), co nie tylko obniża rolę zasady legalności w dziedzinie prawa, w której jej rygorystyczna interpretacja jest najbardziej potrzebna, ale także pozostawia szerokie drzwi do twórczej interpretacji prawa. Przykładem tej niepokojącej, kreatywnej interpretacji jest w tym przypadku sam rząd, który odnosi się do dwóch następujących zadań wykonywanych przez tajne zgromadzenie wywiadowcze za zgodą ministrów na Węgrzech z jednej strony, w celu wykrywania i eliminowania aktów terroryzmu, a z drugiej, w celu znalezienia i uratowania obywateli węgierskich, którzy znaleźli się w kłopotach w obcym kraju. Zaskarżone przepisy mogą mieć wpływ na skarżących jedynie w zakresie, w jakim ustawa nie wyklucza ich z kręgu osób, które w kontekście wykrywania i identyfikacji osoby lub grupy osób potencjalnie związanych z aktem terrorystycznym mogą, wśród osób lub w miejscu lub ośrodku zagrożonym aktem terrorystycznym, zostać dotknięte tajnym gromadzeniem informacji wywiadowczych..."(zob. s. 8 uwag rządu z dnia 31 października 2014 r.). Oznacza to, że każda osoba mająca "potencjalny związek" z aktem terrorystycznym lub miejscem zagrożonym aktem terroryzmu, w tym potencjalne ofiary, może zostać poddana nadzorowi, jak również każda osoba potencjalnie związana z incydentem z Węgrem, który "popadł w kłopoty w obcym kraju"! W uzasadnionej logice bezpieczeństwa rząd stwierdza, że "aspekty bezpieczeństwa narodowego, które mają być ważone, mogą być określone w prawie w bardzo szerokim zakresie, ponieważ w rzeczywistej ocenie aspekty polityki bezpieczeństwa, to znaczy aspekty nie prawne będą miały priorytetowy charakter.... W dziedzinie udzielania zezwoleń na prowadzenie celowego tajnego wywiadu o bezpieczeństwie narodowym nie ma pozytywnego prawa określającego dokładne kryteria, na podstawie których istnieje lub może zostać stworzony system kryteriów, na podstawie których może zostać wydana decyzja sądowa... Dlatego w dziedzinie walki z terroryzmem upoważnienie do gromadzenia tajnych informacji wywiadowczych w celu zapewnienia bezpieczeństwa narodowego jest przyznawane na podstawie systemu kryteriów politycznych, które nie mogą być określone przez prawo...”(patrz str. 12 Uwagi). Podsumowując perspektywę rządu, nadzór tajny państwa to dziedzina polityki i żadna ustawa nie "wychodzi lub może zostać stworzona" w celu ograniczenia tej dziedziny. [↑](#footnote-ref-31)
32. *Iordachi i Inni przeciwko Mołdawii*, nr 25198/02, 10 lutego 2009. Zobacz również moją odrębną opinię w *Draksas*, cytowany powyżej, strona 26, punkt (3), i punkt 27 za podobne braki w prawie litewskim,. [↑](#footnote-ref-32)
33. Krytyka Izby wyrażona w paragrafie 69 wyroku jest całkowicie słuszna, ale niestety Izba nie doszła do logicznego końca. [↑](#footnote-ref-33)
34. Innymi słowy, norma Izby jest nawet niższa niż najniższy stopień podejrzliwości w dobrej wierze lub "wstępnego podejrzenia" (Anfangsverdacht) w prawie karnym. Odwołanie Izby do paragrafów 259 i 261 *Zakharov* wprowadza w błąd, ponieważ Wielka Izba zakwalifikowała "indywidualne podejrzenie", ograniczając je do "uzasadnionego podejrzenia" w paragrafach 260,262 i 263, które Izba postanowiła zignorować. Ponadto odniesienie Izby do "dostatecznej podstawy faktycznej" nie dodaje nic więcej, ponieważ ta "podstawa dowodowa" odnosi się do "materiałów pomocniczych", a nie do stopnia podejrzliwości wymaganego do uzasadnienia zastosowania jakiegokolwiek środka polegającego na tajnym gromadzeniu informacji wywiadowczych. Dalsze dyskusje na temat trzech możliwych stopni podejrzeń w dziedzinie prawa karnego można znaleźć w odrębnej opinii *w Lagutin i in*., cytowany powyżej, str. 38, punkt 9.1). [↑](#footnote-ref-34)
35. Paragraf 78 wyroku. [↑](#footnote-ref-35)
36. *Liberty i Inni przeciwko Zjednoczonemu Królestwu*, nr 58243/00, § 63, 1 lipca 2008, oraz *Weber i Saravia przeciwko Niemcom (dec.)*, nr 54934/00, § 114, 29 czerwca 2006, oba dotyczyły ogólnego "monitorowania strategicznego”. [↑](#footnote-ref-36)
37. Paragraf 12 rezolucji Parlamentu Europejskiego, z dnia 12 marca 2014 r., cytowana powyżej. [↑](#footnote-ref-37)
38. W rzeczywistości Izba używa dwóch “języków”. Paragraf 58 odnosi się do kryterium "konieczności" i wymogów "konieczności", ale później język staje się coraz bardziej wymagający, dodając przymiotnik "rygorystyczny" do słowa "konieczność".. [↑](#footnote-ref-38)
39. *Roman Zakharov*, cytowany powyżej, § 233 (“granice niezbędności w rozumieniu art. 8 ust. 2”) i § 236 (“test niezbędności”, “wspólne zajęcie się wymogami "zgodności z prawem” i "konieczności”). [↑](#footnote-ref-39)
40. Zobacz moją odrębną opinię w *Draksas*, cytowany powyżej, strona 26, punkt (4),oraz moją opinię w *Lagutin i Inni*, cytowany powyżej, strona 36, punkt (6). [↑](#footnote-ref-40)
41. Zobacz moją odrębną opinię w *Draksas*, cytowany powyżej, strona 26, punkt (5). [↑](#footnote-ref-41)
42. W odniesieniu do trzech etapów procedury nadzoru, kiedy nadzór jest zarządzany po raz pierwszy, w czasie jego prowadzenia i po jego zakończeniu, zob. paragraf 233. of *Roman Zakharov*, cytowany powyżej, jak też paragraf 72decyzji nr 32/2013 (XI.22) AB Trybunału Konstytucyjnego, cytowanej w paragrafie 20 niniejszego wyroku. [↑](#footnote-ref-42)
43. *Klass i Inni przeciwko Niemcom*, 6 września 1978, §§ 55 oraz 56, Seria A, nr 28. [↑](#footnote-ref-43)
44. Zob. także moją odrębną opinię w *Draksas*, cytowana powyżej, strona 26, paragraf (6. Tak więc nie mogę się zgodzić z węgierskim Trybunałem Konstytucyjnym, że “Identyfikacja i zwalczanie wysiłków zmierzających do popełnienia czynów mających znaczenie z punktu widzenia zapewnienia suwerenności państwa i ochrony zgodnego z prawem porządku państwa może wykraczać poza sferę poszczególnych przestępstw … Zapobieganie i eliminacja zagrożeń dla bezpieczeństwa narodowego wymaga decyzji politycznych, dlatego decyzje tego rodzaju należą do kompetencji władzy wykonawczej” (paragraf 105 decyzji nr 32/2013 (XI. 22) AB Trybunału Konstytucyjnego, przywołanej w paragrafie 20 wyroku). Nie mogę również zgodzić się z argumentem rządu, że sędziowie nie są mile widziani "ponieważ albo z powodu braku kompetencji, albo braku zewnętrznej - politycznej - politycznej - odpowiedzialności ze strony sądów, albo - w przypadku specjalizacji - ze względu na to, że sądy stają się częścią systemu i ich gotowość do uprzywilejowania interesów bezpieczeństwa narodowego, sądy zazwyczaj akceptują ocenę ryzyka krajowych służb bezpieczeństwa, a zatem kontrola sądowa stanowi jedynie nadzór formalny" (Uwagi rządu dotyczące bezpieczeństwa narodowego z dnia 31 października 2014, strona 11.). [↑](#footnote-ref-44)
45. Mimo że Komitet może żądać informacji w szczególnych przypadkach zgodnie z art. 14 ust. 4 lit. a) ustawy o bezpieczeństwie narodowym, a minister lub dyrektor naczelny w ustalonym terminie udziela odpowiedzi, Komisja nie posiada żadnych uprawnień decyzyjnych w odniesieniu do poszczególnych przypadków.. [↑](#footnote-ref-45)
46. Artykuł 23 ust. 2 ustawy CXI z 2011 r. w sprawie komisarza ds. praw podstawowych. Jest to sprzeczne z zasadą, zgodnie z którą instytucje nadzorcze powinny mieć uprawnienia do wszczynania własnych dochodzeń w obszarach działalności służb wywiadowczych, które wchodzą w zakres ich mandatu, oraz mają dostęp do wszelkich niezbędnych w tym celu informacji. (Zob. zestawienie dobrych praktyk ONZ 2010, przywołane powyżej, paragraf 14, i cytowanym powyżej sprawozdaniu UNHCHR 2014, paragraf 41.). Rzeczywiście w rzeczywistości urząd Rzecznika Praw Obywatelskich nigdy nie zajmował się sprawą dotyczącą nadzoru nad obywatelem (zob. paragraf 18 wyroku i załącznik 2 do uwag skarżących). [↑](#footnote-ref-46)
47. Taka całościowa ocena została dokonana na gruncie prawa europejskiego przez Wielką Izbę w *Roman Zakharov*, cytowany powyżej § 178. Węgierski Trybunał Konstytucyjny zbadał zarówno etap zatwierdzania, jak i postępowania z zebranymi danymi po ustaniu ingerencji i uznał, że ochrona prawa do prywatności jest zadowalająca w świetle gwarancji po etapie zatwierdzania, takich jak parlamentarny nadzór zewnętrzny. Sam rząd odniósł się do tych gwarancji w paragrafach 16-18 swoich uwag. Chociaż w paragrafie 58 wyroku Izba uznała, że “Trybunał jest zobowiązany do zbadania samego tego aktu prawnego i zabezpieczeń wbudowanych w system pozwalający na nadzór tajny”, nie spełniła ona obietnic.. [↑](#footnote-ref-47)
48. W paragrafie 274 cytowanego powyżej wyroku *Roman Zakharov* Trybunał zauważył, że sądy krajowe nie były właściwe do nadzorowania etapu wdrażania tajnego nadzoru, stwierdzając w paragrafie 285, że nadzór tego drugiego etapu sprawowany przez prokuratora jest niewystarczający. [↑](#footnote-ref-48)
49. Wykładnia zaproponowana przez Trybunał Konstytucyjny w paragrafie 138 decyzji nr 32/2013 (XI. 22) AB Trybunału Konstytucyjnego, przytoczona w paragrafie 20 wyroku, wywodząca się z pkt. 43 i 50 ust. 2 lit. e) w związku z pkt. 43 i art. 50 ust. 2 lit. e), wynikająca z prawnego obowiązku usunięcia z urzędu zbędnych danych nie tylko wydaje się wymuszona, ale w rzeczywistości nie rozwiązuje problemu, ponieważ nie podano żadnych konkretnych informacji na temat kompetencji, terminu i procedury usuwania danych zgromadzonych w celu artykułu 7/E (3) Ustawy o Policji. [↑](#footnote-ref-49)
50. Zobacz moją odrębną opinię w *Draksas*, cytowana powyżej, str. 28, za podobne braki w litewskim prawie. Paragraf 255 cytowanego wyżej *Roman Zakharov*, cenzura automatyczna przechowywanych przez sześć miesięcy danych wyraźnie nieistotnych. Wielka izba nie wzięła jednak pod uwagę interesu osoby podlegającej monitorowaniu w powoływaniu się w swojej obronie na rzekomo "nieistotne" dane, jak słusznie stwierdzono w sprawie *Dumitru Popescu przeciwko Rumunii (nr 2)*, nr 71525/01, § 78,26 kwietnia 2007 r.. [↑](#footnote-ref-50)
51. *Integracja Europejska i Prawa Człowieka i Ekimzhiev przeciwko Bułgarii*, nr 62540/00, § 16, 28 czerwca 2007. [↑](#footnote-ref-51)
52. Zobacz moją opinię w *Draksas*, cytowany powyżej, strona 26, punkt (8). [↑](#footnote-ref-52)
53. *Klass i Inni*, cytowany powyżej, §§ 55 i 56. Zobacz również moją opinię w *Draksas*, cytowany powyżej, strona 26, punkt (9), i strona 29 za podobne braki w prawie litewskim. [↑](#footnote-ref-53)
54. Zobacz również moją opinię w *Draksas*, cytowany powyżej, strona 26, punkt (10). W przywołanej powyżej rezolucji Zgromadzenia Parlamentarnego nr 1954 (2013) potwierdzono, że nie należy stosować środków takich jak nakazy przechwycenia lub działania dotyczące komunikacji lub korespondencji dziennikarzy lub ich pracodawców, nakazy lub działania nadzorcze dotyczące dziennikarzy, ich kontaktów lub pracodawców, jeżeli ich celem jest obejście prawa dziennikarzy do nieujawniania informacji identyfikujących źródło. Komisja Wenecka bardzo niedawno podkreśliła "szczególnie problematyczny" charakter przechwytywania uprzywilejowanych komunikatów za pomocą tajnego wywiadu prawników, księży lub dziennikarzy i dała przykład tajnego nadzoru nad dziennikarzami w celu zidentyfikowania ich źródeł (aktualizowane sprawozdanie z 2007 r. przez Komisję Wenecką, przywołane powyżej, pkt. 18 i 106-108). [↑](#footnote-ref-54)
55. Potwierdzają to nieistnienie skarg do Komisji Bezpieczeństwa Narodowego (załącznik 1 do uwag skarżących, potwierdzony uwagami rządu z dnia 14 stycznia 2015 r.). [↑](#footnote-ref-55)
56. W Rosji ogólne środki odwoławcze były dostępne jedynie dla osób będących w posiadaniu informacji o danym środku nadzoru, a zatem ich skuteczność została osłabiona przez brak wymogu powiadamiania podmiotu tego środka w dowolnym momencie (zob. cytowany powyżej *Roman Zakharov*, § 298, *wcześniej Stowarzyszenie Integracji Europejskiej i Praw Człowieka* oraz cytowany powyżej *Ekimdzhiev*, § 100). [↑](#footnote-ref-56)
57. Zobacz interpretację Trybunału Konstytucyjnego tego przepisu, w paragrafie 138 swojej decyzji, nr 32/2013 (XI.22) AB, cytowana powyżej w paragrafie 20 wyroku. [↑](#footnote-ref-57)
58. Nie mogę zatem zgodzić się ze stwierdzeniem Trybunału Konstytucyjnego, że "skoro tajne gromadzenie informacji wywiadowczych z definicji wyklucza możliwość skutecznego środka odwoławczego..." (zob. paragraf 72 decyzji nr 32/2013 (XI. 22) AB Trybunału Konstytucyjnego, cytowanej w pkt. 20 wyroku). [↑](#footnote-ref-58)
59. Samuel Warren i Louis Brandeis, “Prawo do prywatności”, Harvard Law Review, wolumen IV, nr 5, 15 grudnia 1890, s. 196. [↑](#footnote-ref-59)
60. *Rotaru przeciwko Rumunii* [WI], nr 28341/95, § 59 z dnia 5 maja 2000 r., parafrazowanie w *Klass i in.,* cytowany powyżej, § 49:"Mając świadomość niebezpieczeństwa, jakie ustawa ta niesie ze sobą podważając lub nawet niszcząc demokrację ze względu na jej obronę, Trybunał stwierdza, że Umawiające się Państwa nie mogą w imieniu walki z szpiegostwem i terroryzmem podejmować żadnych środków, jakie uznają za stosowne.” [↑](#footnote-ref-60)
61. Jest to w szczególności niepokojące, jeżeli weźmie się pod uwagę, że w ciągu ostatnich lat, kilka organizacji zajmujących się ochroną prywatności i prawami cyfrowymi wskazywało na dowody, że władze węgierskie zakupiły potencjalnie inwazyjne technologie nadzoru (Wolność domu, Wolność Internetu, sprawozdanie na temat Węgier, 2015, strona 15). [↑](#footnote-ref-61)