



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

© Naczelny Sąd Administracyjny, www.nsa.gov.pl [Translation already published on the official website of the Polish Supreme Administrative Court] Permission to re-publish this translation has been granted by the Polish Supreme Administrative Court for the sole purpose of its inclusion in the Court's database HUDOC

© Naczelny Sąd Administracyjny, www.nsa.gov.pl [Tłumaczenie zostało już opublikowane na oficjalnej stronie Naczelnego Sądu Administracyjnego] Zezwolenie na publikację tego tłumaczenia zostało udzielone przez Naczelny Sąd Administracyjny wyłącznie w celu zamieszczenia w bazie Trybunału HUDOC

PIĄTA SEKCJA

SPRAWA BREYER PRZECIWKO NIEMCOM
(Skarga nr 50001/12)

WYROK
[wyciąg]

Art. 8 • Poszanowanie życia prywatnego • Spoczywający na usługodawcach obowiązek przechowywania danych osobowych użytkowników przedpłaconych kart SIM do telefonów komórkowych i udostępniania ich na żądanie władz • Ingerencja dotycząca ograniczonego zbioru danych • Wyszukiwanie danych przez władze połączone z odpowiednimi zabezpieczeniami • Kwestionowane przechowywanie proporcjonalne do uprawnionych celów ochrony bezpieczeństwa narodowego i zwalczania przestępczości

STRASBURG

30 stycznia 2020 r.

OSTATECZNY

07/09/2020 r.

Wyrok ten stał się ostateczny na podstawie art. 44 § 2 Konwencji. Może podlegać korekcie redakcyjnej.

W sprawie Breyer przeciwko Niemcom,

Europejski Trybunał Praw Człowieka (czwarta sekcja), zasiadając jako Izba w składzie:

Yonko Grozev, *Przewodniczący,*

Angelika Nußberger,

Síofra O’Leary,

Carlo Ranzoni,

Mārtiņš Mits,

Lətif Hüseynov,

Lado Chanturia, *sędziowie,*

oraz Claudia Westerdiek, *Kancelarz Sekcji,*

obradując na posiedzeniu niejawnym w dniu 3 grudnia 2019 roku,

wyduje następujący wyrok, który został przyjęty w tym dniu:

POSTĘPOWANIE

1. Sprawa wywodzi się ze skargi (nr 50001/12) przeciwko Republice Federalnej Niemiec, wniesionej do Trybunału na podstawie art. 34 Konwencji o ochronie praw człowieka i podstawowych wolności („Konwencja”) przez dwóch obywateli niemieckich, panów Patricka Breyera i Jonasa Breyera („skarżący”) w dniu 27 lipca 2012 r.

2. Rząd niemiecki („Rząd”) był reprezentowany przez swoich Pełnomocników, pana H.-J. Behrensa i panią K. Behr z Federalnego Ministerstwa Sprawiedliwości i Ochrony Konsumentów.

3. Skarżący zarzucili na podstawie art. 8 i 10, że pewne ich dane osobowe, jako użytkowników przedpłaconych kart SIM do telefonów komórkowych, były przechowywane przez ich odpowiednich dostawców usług w związku z obowiązkiem prawnym przewidzianym w art. 111 ustawy telekomunikacyjnej.

4. W dniu 21 marca września 2016 r. skarga została zakomunikowana Rządowi.

5. Pisemne uwagi otrzymano od Privacy International i ARTICLE 19, którym Wiceprzewodniczący udzielił zgody na interwencję w charakterze stron trzecich (art. 36 ust. 2 Konwencji i Reguła 44 § 2 Regulaminu Trybunału).

FAKTY

« [Paragrafy 5 – 58 wyroku pominięto i zastąpiono tłumaczeniem poniższego streszczenia przygotowanego przez Kancelarię Europejskiego Trybunału Praw Człowieka

Streszczenie stanu faktycznego¹:

W 2004 r. ustawa telekomunikacyjna nałożyła na dostawców usług obowiązek zbierania różnych danych osobowych wszystkich ich klientów i przechowywania ich wraz z przydzielonym numerem telefonu, nawet jeśli nie było to konieczne do celów rozliczeń lub z innych powodów wynikających z umowy.

Pobrania i przekazania danych mogły żądać różne organy publiczne bez wymogu przedstawienia nakazu sądu i powiadomienia osób zainteresowanych. Wnioski o pobranie danych mogły być pod pewnymi warunkami zautomatyzowane i skutkować przedłożeniem list opartych jedynie na podobieństwie nazwisk lub numerów (zapytania o dane częściowe). Takie wnioski o informacje były dopuszczalne, gdy były uznane za konieczne „w celu ścigania przestępstw karnych lub administracyjnych, zapobieżenia niebezpieczeństwu oraz wykonywania zadań wywiadowczych”.

Skarżący nabyli przedpłacone karty SIM, a zatem przy aktywacji tych kart byli zobowiązani do zarejestrowania swoich nazwisk, adresów oraz dat urodzenia u swoich dostawców usług. Złożyli odwołanie do Federalnego Trybunału Konstytucyjnego, ale bez powodzenia.

Aby zachować ten sam temporalny zakres badania sprawy co wskazany wyżej sąd krajowy, Trybunał zbadał zaskarżone przepisy według stanu obowiązującego w dniu 1 stycznia 2008 r.

PRAWO

ZARZUT NARUSZENIA ART. 8 I ART. 10 KONWENCJI

6. Skarżący zarzucili, że pewne ich dane osobowe, jako użytkowników przedpłaconych kart SIM do telefonów komórkowych, były przechowywane przez odpowiednich dostawców ich usług telekomunikacyjnych w związku z obowiązkiem prawnym przewidzianym

¹ Źródło: Nota informacyjna na temat orzecznictwa Trybunału nr 236, styczeń 2020 r. (*Information Note. Case-law of the European Court of Human Rights No. 236, January 2020 / Note d'information sur la jurisprudence de la Cour 236 / Janvier 2020*)

w art. 111 ustawy telekomunikacyjnej. Powołali się na swoje prawo do poszanowania życia prywatnego i korespondencji przewidziane w art. 8 Konwencji oraz na wolność wyrażania opinii przewidzianą w art. 10 Konwencji, które w zakresie istotnym dla niniejszej sprawy brzmią następująco:

Artykuł 8

„1. Każdy ma prawo do poszanowania swojego życia prywatnego ... 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 ..., ochronę porządku i zapobieganie przestępstwom...”

Artykuł 10

„1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. ...

2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego ... lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu...”

A. Zakres skargi i ocena Trybunału

1. Prawa wynikające z Konwencji podlegające ocenie

7. Na wstępie Trybunał zauważa, że skarżący powołali się na art. 8 (prawo do poszanowania życia prywatnego i korespondencji) oraz art. 10 (prawo do anonimowej łączności jako aspekt wolności wyrażania opinii). Jednak zauważa również, że przed Trybunałem skarżący zakwestionowali jedynie zgodność art.111 ustawy telekomunikacyjnej z Konwencją. Nie skarżyli się wyraźnie na art. 112 lub 113 tej ustawy, które również były przedmiotem ich skargi przed Federalnym Trybunałem Konstytucyjnym, ani na żadne inne środki dotyczące nadzoru nad łącznością telefoniczną lub jej przechwytywania. Nie oznacza to jednak, że te inne przepisy ustawy telekomunikacyjnej nie okażą się istotne przy ocenie proporcjonalności ingerencji będącej przedmiotem skargi oraz jej funkcjonowania w praktyce (zob. paragrafy 97-101 poniżej).

8. Art. 111 ustawy telekomunikacyjnej dotyczy jedynie przechowywania danych abonenta, a mianowicie numeru telefonu, nazwiska i adresu, daty urodzenia oraz daty zawarcia umowy. Przepis ten nie obejmuje danych o ruchu, danych o lokalizacji ani danych ujawniających treść łączności. Ponadto skarżący nie zarzucili, że ich przekazy zostały przechwycone lub

że ich przekazy telekomunikacyjne zostały poddane jakimkolwiek innym środkom nadzoru. Ingerencja będąca przedmiotem skargi dotyczy przechowywania wyżej opisanego zbioru danych oraz możliwości dostępu władz krajowych do tego zbioru danych w pewnych określonych okolicznościach. Dlatego też, choć Trybunał ma na uwadze okoliczności przedmiotowego przechowywania danych oraz bliskości łączności telefonicznej i prawa do korespondencji, uważa, że kluczowym aspektem skargi skarżących jest przechowywanie ich danych osobowych, a nie jakakolwiek szczególna ingerencja w ich korespondencję lub wolność wyrażania opinii.

9. Zatem w niniejszej sprawie Trybunał nie jest wzywany do rozstrzygnięcia, czy i w jakim zakresie można uznać, że art. 10 Konwencji gwarantuje użytkownikom usług telekomunikacyjnych prawo do anonimowości (zob. w odniesieniu do interesu użytkowników Internetu w nieujawnianiu ich tożsamości, *Delfi AS przeciwko Estonii* [WI], nr 64569/09, § 147, 16 czerwca 2015 r.) oraz jak to prawo musiałoby być zrównoważone w stosunku do innych imperatywów (zob. *mutatis mutandis*, *K.U. przeciwko Finlandii*, nr 2872/02, § 49, 2 grudnia 2008 r.).

10. Podsumowując, Trybunał uznaje za właściwe zbadanie skarg skarżących wyłącznie pod kątem prawa do poszanowania życia prywatnego przewidzianego w art. 8 Konwencji.

2. Zakres czasowy oceny

11. Trybunał zauważa, że dane abonenckie skarżących były tymczasowo przechowywane przez dostawcę usług telekomunikacyjnych od momentu rejestracji ich kart SIM. Zauważa również, że art. 111 ustawy telekomunikacyjnej został zmieniony w 2007 r. i 2016 r. Zauważa jednak, że w swoim wyroku z dnia 24 stycznia 2012 r. Federalny Trybunał Konstytucyjny zbadał ustawę telekomunikacyjną w brzmieniu obowiązującym w dniu 1 stycznia 2008 r., oraz że postępowanie dotyczące późniejszej nowelizacji ustawy telekomunikacyjnej z 2016 r. nadal toczy się przed Federalnym Trybunałem Konstytucyjnym (zob. paragrafy 11 i 28 powyżej). Trybunał zbada zatem odpowiednie przepisy w brzmieniu obowiązującym w dniu 1 stycznia 2008 r.

B. Dopuszczalność

12. Trybunał stwierdza, że skarga nie jest w sposób oczywisty nieuzasadniona w rozumieniu art. 35 ust. 3 lit. a Konwencji. Ponadto stwierdza, że nie jest ona niedopuszczalna z jakichkolwiek innych powodów. Należy ją zatem uznać za dopuszczalną.

C. Meritum skargi

1. Oświadczenia stron

a) Skarżący

13. Skarżący twierdzili, że obowiązek przechowywania ich danych osobowych na podstawie art. 111 ustawy telekomunikacyjnej naruszył ich prawo do prywatności, ponieważ zmusił ich do ujawnienia swoich danych osobowych, które następnie były przechowywane. Ingerencja ta nie była uzasadniona, w szczególności dlatego, że była nieproporcjonalna i nie była konieczna w społeczeństwie demokratycznym. Po pierwsze, przepis ten nie był odpowiednim instrumentem, ponieważ proces identyfikacji można było łatwo obejść, podając fałszywe nazwiska lub używając skradzionych, używanych lub zagranicznych kart SIM. Nie był on również konieczny, ponieważ identyfikacja użytkowników telefonów komórkowych podejrzanych o popełnienie przestępstwa może być łatwo dokonana za pomocą innych środków dochodzeniowych. W związku z tym zmiana art. 111 ustawy telekomunikacyjnej nie doprowadziła do zmniejszenia przestępczości.

14. Zdaniem skarżących ingerencja była bardzo poważna, gdyż stanowiła masowe zapobiegawcze przechowywanie danych osobowych każdego, kto korzystał z usług telekomunikacji. Przepis nie zawierał żadnych przesłanek do przechowywania, ale dotyczył ogólnie wszystkich użytkowników telefonów komórkowych. Dotknięte nim osoby w zdecydowanej większości były niewinne i nie stanowiły żadnego zagrożenia ani ryzyka dla bezpieczeństwa publicznego lub narodowego. W tym względzie skarżący twierdzili, że według Federalnej Agencji ds. Sieci liczba przeszukiwanych zbiorów danych w ramach zautomatyzowanej procedury przewidzianej w art. 112 ustawy telekomunikacyjnej wzrosła z 26,62 mln w 2008 r. do 34,83 mln w 2015 r. Co więcej, przepis ten nie rozróżniał również „normalnej” łączności od łączności szczególnie chronionej przez Konwencję, np. między prawnikiem i jego klientem lub lekarzem i jego pacjentem. Ponadto, przechowywanie danych zwiększało ryzyko niewłaściwego wykorzystania i wycieku danych, a tym samym ryzyko oszustwa dotyczącego tożsamości.

b) Rząd

15. Rząd przyznał, że art. 111 ustawy telekomunikacyjnej stanowił ingerencję w prawo skarżących do życia prywatnego. Zobowiązywał on dostawców ich usług do przechowywania ich danych osobowych. Rząd podkreślił, że nie były przechowywane żadne tzw. dane o ruchu - czyli dane pochodzące z procesu łączności - a jedynie wyżej wymienione informacje o abonencie (zob. paragraf 61 powyżej). Ponadto, art. 111 należało czytać w powiązaniu z art. 112 i 113 ustawy telekomunikacyjnej oraz z dalszymi

przepisami ograniczającymi dostęp do przechowywanych danych, ponieważ organy wyszukujące dane abonentów musiały mieć do tego ustawową podstawę.

16. Ta ograniczona ingerencja była uzasadniona uprawnionymi celami bezpieczeństwa publicznego, ochrony porządku i zapobiegania przestępstwom oraz ochrony praw i wolności innych osób i była odpowiednim instrumentem do ich realizacji, ponieważ zapewniała organom bezpieczeństwa możliwość powiązania numerów telefonów komórkowych przedpłaconych kart SIM z konkretnymi osobami. Możliwość ta przyczyniłaby się do skutecznego egzekwowania prawa i służyłaby zapobieganiu zagrożeniom. Możliwość obejścia tego przepisu została dodatkowo ograniczona nowelizacją z 2016 roku (zob. paragraf 28 powyżej).

17. Przedmiotowy przepis był również zgodny z wymogami ochrony danych osobowych ustanowionymi przez Trybunał w sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu* ([WI], nr 30562/04 i 30566/04, § 103, ETPC 2008). Ograniczał on ilość danych do tych, które były bezwzględnie konieczne do identyfikacji. Okres przechowywania danych był jasno określony i ograniczony do maksymalnego okresu nieprzekraczającego okresu niezbędnego ze względu na realizowany cel. Ponadto art. 112 i 113 ustawy telekomunikacyjnej w powiązaniu ze szczególnymi przepisami dotyczącymi wyszukiwania danych stanowiły skuteczne zabezpieczenia przed nadużyciami.

18. Należało również wziąć pod uwagę fakt, że margines oceny przyznany państwom członkowskim był stosunkowo szeroki, nie tylko dlatego, że władze niemieckie musiały zachować równowagę pomiędzy różnymi konkurującymi prawami i obowiązkami chronionymi przez Konwencję (powołały się na sprawę *Evans przeciwko Zjednoczonemu Królestwu* [WI], nr 6339/05, § 77, 10 kwietnia 2007 r.), ale również dlatego, że nie istniał europejski konsensus co do obowiązku przechowywania danych abonenta przy nabywaniu przedpłaconych kart SIM do telefonów komórkowych. Podsumowując, przechowywanie bardzo minimalnego zbioru danych, chronionych kilkoma gwarancjami proceduralnymi, było proporcjonalne w zasadniczym interesie bezpieczeństwa publicznego oraz ochrony porządku i zapobiegania przestępstwom.

c) Interwenienci uboczni

19. Interwenienci uboczni, Privacy International i ARTICLE 19, podkreślili znaczenie anonimowości i anonimowych wypowiedzi dla społeczeństwa demokratycznego oraz praw obywateli do prywatności i wolności wyrażania opinii. Ta podstawowa rola była coraz częściej uznawana przez sądy krajowe i organizacje międzynarodowe, takie jak Organizacja Narodów Zjednoczonych i Rada Europy. Ponadto, sam Trybunał potwierdził znaczenie anonimowości w sprawie *Delfi AS*

przeciwko Estonii (cyt. powyżej, §§ 147-48). Co więcej, wskazali oni na fakt, że sądy w Europie coraz częściej uznają, że blankietowe, masowe zatrzymywanie informacji identyfikacyjnych i danych dotyczących ruchu jest nieproporcjonalne do niewątpliwie ważnej walki z poważną przestępczością. Potwierdził to również TSUE w wyroku w sprawie *Digital Rights Ireland i Seitlinger i Inni* (zob. paragraf 51 powyżej).

2. Ocena Trybunału

a) Zasady ogólne

20. Trybunał przypomina, że życie prywatne jest szerokim pojęciem niepodlegającym wyczerpującej definicji. Art. 8 chroni między innymi prawo do tożsamości i rozwoju osobistego oraz prawo do nawiązywania i rozwijania stosunków z innymi ludźmi i światem zewnętrznym. Istnieje zatem strefa stosunków osoby z innymi, nawet w kontekście publicznym, która może wchodzić w zakres „życia prywatnego” (zob. *Uzun przeciwko Niemcom*, nr 35623/05, § 43, 2 września 2010 r.).

21. W kontekście danych osobowych Trybunał wskazał, że termin „życie prywatne” nie może być interpretowany zawężająco. Stwierdził, że szeroka interpretacja odpowiada tej zawartej w Konwencji o ochronie danych, której celem jest „zapewnienie każdej osobie fizycznej ... poszanowania jej praw i podstawowych wolności na terytorium każdej ze stron Konwencji, a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych”(art. 1), przy czym takie dane osobowe zdefiniowano jako „każdą informację dotyczącą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować” (art. 2) (zob. *Amann przeciwko Szwajcarii* [WI], nr 27798/95, § 65, 16 lutego 2000 r.).

22. Z utrwalonego orzecznictwa Trybunału wynika ponadto, że w przypadku, gdy dojdzie do zestawienia danych dotyczących konkretnej jednostki, przetwarzania lub wykorzystywania danych osobowych lub publikowania określonych materiałów w sposób wykraczający lub w stopniu wykraczającym poza normalnie przewidywalny, pojawiają się względy dotyczące życia prywatnego. Art. 8 Konwencji zapewnia zatem prawo do decydowania o wykorzystywaniu własnych informacji, umożliwiając jednostkom powoływanie się na ich prawo do prywatności w odniesieniu do danych, które, choć neutralne, są gromadzone, przetwarzane i rozpowszechniane zbiorczo oraz w takiej formie lub w taki sposób, że mogą zostać zaangażowane ich prawa wynikające z art. 8 (zob. *Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii* [WI], nr 931/13, §§ 136-37, 27 czerwca 2017 r., z dalszymi odniesieniami).

23. Trybunał zauważa, że chociaż zbadał już szeroki zakres ingerencji w prawo do życia prywatnego na podstawie art. 8 Konwencji w wyniku przechowywania, przetwarzania i wykorzystywania danych osobowych - na

przykład wykorzystanie nadzoru za pośrednictwem GPS w dochodzeniach karnych (zob. *Uzun*, cyt. powyżej, oraz *Ben Faiza przeciwko Francji*, nr 31446/12, 8 lutego 2018 r.), ujawnianie informacji identyfikacyjnych organom ścigania przez dostawców usług telekomunikacyjnych (zob. *K.U. przeciwko Finlandii*, cyt. powyżej, oraz *Benedik przeciwko Słowenii*, nr 62357/14, 24 kwietnia 2018 r.), bezterminowe zatrzymywanie odcisków palców, próbek komórek i profili DNA po zakończeniu postępowania karnego (zob. *S. i Marper*, cyt. powyżej), pomiar (tzw. *metering*) lub gromadzenie danych o użytkowaniu lub ruchu (zob. *Malone przeciwko Zjednoczonemu Królestwu*, 2 sierpnia 1984 r., Seria A nr 82, oraz *Copland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, 3 kwietnia 2007 r.) lub umieszczanie przestępców seksualnych w zautomatyzowanej krajowej bazie sądowej po skazaniu za gwałt (zob. *B.B. przeciwko Francji*, nr 5335/06, 17 grudnia 2009 r.; *Gardel przeciwko Francji*, nr 16428/05, ETPC 2009; oraz *M.B. przeciwko Francji*, nr 22115/06, 17 grudnia 2009 r.) - żadna z poprzednich spraw nie dotyczyła przechowywania zbioru danych takiego jak w niniejszej sprawie.

24. Obowiązek, podobny jak w art. 111 ustawy telekomunikacyjnej, tworzenia baz danych przechowujących informacje (imię, nazwisko patronimiczne i rodowe, adres zamieszkania i numer paszportu dla osób fizycznych) o wszystkich abonentach oraz zapewnienia organom ścigania zdalnego dostępu do baz danych był wprawdzie częścią systemu tajnego nadzoru, który Trybunał rozpatrywał w sprawie *Roman Zakharov przeciwko Rosji* ([WI], nr 47143/06, §§ 132-33 i 269-70, ETPC 2015). Jednak, biorąc pod uwagę dalsze możliwości, jakimi dysponują władze rosyjskie w zakresie przechwytywania przekazów telekomunikacyjnych, sam obowiązek przechowywania informacji o abonentach i zapewnienia zdalnego dostępu do tej bazy danych nie był dla Trybunału decydujący przy stwierdzeniu naruszenia art. 8 w tamtej sprawie.

25. W wyroku w sprawie *S. i Marper* (cyt. powyżej, § 103) Trybunał stwierdził, co następuje:

„Ochrona danych osobowych ma podstawowe znaczenie dla korzystania przez osobę z prawa do poszanowania życia prywatnego i rodzinnego, zagwarantowanego w art. 8 Konwencji. Prawo krajowe musi zapewnić odpowiednie zabezpieczenia, aby zapobiec wszelkiemu takiemu wykorzystaniu danych osobowych, które może być niezgodne z gwarancjami określonymi w tym artykule Potrzeba takich zabezpieczeń jest tym większa, gdy chodzi o ochronę danych osobowych podlegających automatycznemu przetwarzaniu, zwłaszcza gdy dane te są wykorzystywane do celów policyjnych. Prawo krajowe powinno w szczególności zapewnić, by takie dane były rzeczowe, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone oraz by były przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego dane te zgromadzono (zob. art. 5 Konwencji o ochronie danych osobowych ... [w paragrafie 47 powyżej]). Prawo krajowe musi również zapewniać odpowiednie gwarancje, żeby zatrzymane dane osobowe były skutecznie chronione przed niewłaściwym wykorzystaniem i

nadużyciami (zob. zwłaszcza art. 7 Konwencji o ochronie danych [w paragrafie 47 powyżej])"

26. Trybunał stwierdził, że przy wyważeniu interesu pozwanego Państwa w ochronie jego bezpieczeństwa narodowego za pomocą tajnych środków nadzoru z powagą ingerencji w prawo skarżącego do poszanowania jego życia prywatnego, władze krajowe korzystają z pewnego marginesu oceny przy wyborze środków służących osiągnięciu uprawnionego celu ochrony bezpieczeństwa narodowego. Jednak margines ten podlega nadzorowi europejskiemu, obejmującemu zarówno ustawodawstwo, jak i decyzje je stosujące (zob. *Roman Zakharov*, cyt. powyżej, § 232; *Liblik i Inni przeciwko Estonii*, nr 173/15 i 5 Innych, § 131, 28 maja 2019 r.; oraz *Szabó i Vissy przeciwko Węgrom*, nr 37138/14, § 57, 12 stycznia 2016 r.).

27. Szerokość marginesu oceny jest różna i zależy od wielu czynników, w tym od charakteru przedmiotowego prawa konwencyjnego, jego znaczenia dla jednostki, charakteru ingerencji i celu, do którego zmierza ingerencja. Margines będzie tym węższy, im zagrożone prawo jest ważniejsze dla faktycznego korzystania przez daną jednostkę z praw osobistych lub podstawowych. Jeśli jednak w państwach członkowskich Rady Europy nie ma zgody co do względnego znaczenia przedmiotowego interesu lub co do najlepszego sposobu jego ochrony, margines będzie szerszy (zob. *S. i Marper*, cyt. powyżej, § 102).

b) Zastosowanie powyższych zasad w niniejszej sprawie

(i) Istnienie ingerencji

28. Strony nie kwestionują, że obowiązek przechowywania przez dostawców usług danych osobowych zgodnie z art. 111 ustawy telekomunikacyjnej ingerował w prawo skarżących do poszanowania ich życia prywatnego, ponieważ ich dane osobowe były przechowywane. W związku z tym Trybunał przypomina, że samo przechowywanie danych dotyczących życia prywatnego jednostki stanowi ingerencję w rozumieniu art. 8 Konwencji (zob. *Leander przeciwko Szwecji*, 26 marca 1987 r., § 48, Seria A nr 116). Ponadto zwraca uwagę na stwierdzenie Federalnego Trybunału Konstytucyjnego, że zakres ochrony prawa do decydowania o wykorzystywaniu własnych informacji w prawie krajowym nie był ograniczony do informacji, które z samej swojej natury były wrażliwe, oraz że w świetle możliwości przetwarzania i łączenia nie istnieje żaden element danych osobowych, który sam w sobie - to znaczy niezależnie od kontekstu jego wykorzystania - byłby nieistotny (zob. § 122 wyroku Federalnego Trybunału Konstytucyjnego cyt. w paragrafie 14 powyżej).

(ii) Uzasadnienie ingerencji

29. Trybunał przypomina, że ingerencja w prawo skarżącego do poszanowania jego życia prywatnego narusza art. 8, chyba że jest „zgodna z ustawą”, jest uzasadniona co najmniej jednym z uprawnionych celów, o których mowa w ust. 2, a ponadto jest „konieczna w demokratycznym społeczeństwie” dla osiągnięcia tych celów (zob. *M.N. i inni przeciwko San Marino*, nr 28005/12, § 71, 7 lipca 2015 r., z dalszymi odniesieniami).

(α) „Zgodna z ustawą”

30. Zgodnie z utrwalonym orzecznictwem Trybunału wymóg, aby ingerencja była „zgodna z ustawą” nie oznacza jedynie, że dany środek powinien mieć jakąś podstawę w prawie krajowym, ale również, że prawo powinno być dostępne dla zainteresowanej jednostki i przewidywalne co do jego skutków. W kontekście m.in. przechowywania danych osobowych niezbędne jest istnienie jasnych, szczegółowych zasad regulujących minimalne zabezpieczenia dotyczące m.in. czasu trwania, przechowywania, wykorzystania, dostępu osób trzecich, procedur zachowania integralności i poufności danych oraz procedur ich niszczenia (zob. *S. i Marper*, cyt. powyżej, § 99, z dalszymi odniesieniami)

31. Trybunał stwierdza, że przechowywanie danych osobowych skarżących przy nabywaniu kart SIM do telefonów komórkowych, miało miejsce na podstawie art. 111 ustawy telekomunikacyjnej, co było, w zakresie dotyczącym ilości przechowywanych danych, wystarczająco jasne i przewidywalne. Ponadto, czas przechowywania był wyraźnie uregulowany, a techniczna strona przechowywania była, przynajmniej po wydaniu odpowiedniego rozporządzenia i dyrektywy technicznej, jasno określona.

32. Jeśli chodzi o zabezpieczenia, dostęp osób trzecich i dalsze korzystanie z przechowywanych danych, art. 111 ustawy telekomunikacyjnej należy czytać w powiązaniu z jej art. 112 i 113 oraz, zgodnie z analogią „podwójnych drzwi” stosowaną przez Federalny Trybunał Konstytucyjny (zob. § 123 wyroku Federalnego Trybunału Konstytucyjnego cyt. w paragrafie 14 powyżej), w powiązaniu z odpowiednią podstawą prawną dla indywidualnych wniosków o udzielenie informacji. Trybunał uważa jednak, że kwestie przewidywalności oraz tego, czy w tych przepisach zawarto wystarczająco szczegółowe informacje, są w niniejszej sprawie ściśle związane z szerszymi zagadnieniami dotyczącymi tego, czy ingerencja była konieczna w demokratycznym społeczeństwie i proporcjonalna. Dlatego też oceni je dogłębniej, gdy przejdzie do tych kwestii (zob. paragrafy 88-110 poniżej).

(β) Uprawniony cel

33. Uwzględniając kontekst przedmiotowego przechowywania danych, a w szczególności cele wniosków o udzielenie informacji oraz organy

uprawnione do ich składania na mocy art. 112 i 113 ustawy telekomunikacyjnej, Trybunał przyjmuje argument Rządu, że ingerencja realizowała uzasadnione cele bezpieczeństwa publicznego, zapobiegania zakłóceniom porządku lub przestępczości oraz ochrony praw i wolności innych osób.

34. W związku z tym Trybunał zwraca uwagę na wyjaśnienie Federalnego Trybunału Konstytucyjnego zawarte w jego wyroku, że dostęp do przechowywanych informacji „służy zapobieganiu zagrożeniom, ściganiu przestępstw lub wykroczeń o charakterze administracyjnym oraz wykonywaniu obowiązków wywiadowczych” (zob. § 176 wyroku Federalnego Trybunału Konstytucyjnego cyt. w paragrafie 21 powyżej). Cele te są dodatkowo podkreślone w ustawie telekomunikacyjnej, która stanowi, że wnioski o udzielenie informacji są dopuszczalne w zakresie, w jakim są one konieczne do ścigania przestępstw i wykroczeń o charakterze administracyjnym, zapobiegania zagrożeniom oraz wykonywania zadań wywiadowczych (zob. paragraf 31 powyżej).

(γ) „Konieczna w demokratycznym społeczeństwie”

35. Ingerencja będzie uznana za „konieczną w demokratycznym społeczeństwie” dla osiągnięcia uprawnionego celu, jeśli odpowiada na „nagłą potrzebę społeczną” i jeśli jest proporcjonalna do realizowanego uprawnionego celu. Trybunał stwierdza, że walka z przestępczością, a w szczególności z przestępczością zorganizowaną i terroryzmem, która jest jednym z wyzwań stojących przed dzisiejszymi społeczeństwami europejskimi, utrzymanie bezpieczeństwa publicznego i ochrona obywateli stanowią „nagłe potrzeby społeczne” (por., *mutatis mutandis*, *Szabó i Vissy*, cyt. powyżej, § 68, oraz *Ramda przeciwko Francji*, nr 78477/11, § 96, 19 grudnia 2017 r.). Uznaje również, że nowoczesne środki telekomunikacji i zmiany w zachowaniach komunikacyjnych wymagają dostosowania narzędzi dochodzeniowych dla organów ścigania i organów bezpieczeństwa narodowego (zob. *S. i Marper*, cyt. powyżej, § 105).

36. Trybunał zauważa, że Rząd dowodził, iż możliwość powiązania numerów telefonów komórkowych przedpłaconych kart SIM z konkretnymi osobami była konieczna dla skutecznego egzekwowania prawa i zapobiegania zagrożeniom. Skarżący zakwestionowali jednak skuteczność art. 111 ustawy telekomunikacyjnej, ponieważ nie było empirycznych dowodów na to, że obowiązkowa rejestracja doprowadziła do zmniejszenia przestępczości. Ponadto argumentowali, że proces identyfikacji można było łatwo obejść, podając fałszywe nazwiska lub używając skradzionych, używanych lub zagranicznych kart SIM.

37. Trybunał zauważa, że wstępna rejestracja abonentów telefonów komórkowych zdecydowanie upraszcza i przyspiesza dochodzenia prowadzone przez organy ścigania, a tym samym może przyczynić się do skutecznego egzekwowania prawa i zapobiegania zakłóceniom porządku

lub przestępczości. Ponadto Trybunał uważa, że istnienie możliwości obejścia obowiązków prawnych nie może stanowić powodu do zakwestionowania ogólnej użyteczności i skuteczności przepisu prawnego. Wreszcie Trybunał przypomina, że w kontekście bezpieczeństwa narodowego władze krajowe korzystają z pewnego marginesu oceny przy wyborze środków służących osiągnięciu uprawnionego celu i zauważa, że zgodnie z raportem prawnoporównawczym nie ma konsensusu między państwami członkowskimi co do zatrzymywania informacji abonenckich klientów przedpłaconych kart SIM (zob. paragraf 58 powyżej). Uwzględniając ten margines oceny, Trybunał przyjął, że obowiązek przechowywania informacji abonenckich na podstawie art. 111 ustawy telekomunikacyjnej był, co do zasady, właściwą odpowiedzią na zmiany w zachowaniach komunikacyjnych i w środkach telekomunikacji.

38. Pozostaje jednak pytanie, czy ingerencja ta była proporcjonalna i zapewniała właściwą równowagę między konkurującymi interesami publicznymi i prywatnymi.

39. Na wstępie Trybunał musi ustalić poziom ingerencji w prawo skarżących do życia prywatnego. W tym zakresie Trybunał zgadza się z Federalnym Trybunałem Konstytucyjnym (zob. § 138-39 wyroku Federalnego Trybunału Konstytucyjnego cyt. w paragrafie 15 powyżej), że przechowywany był jedynie ograniczony zbiór danych. Dane te nie zawierały żadnych wysoce osobistych informacji ani nie pozwalały na tworzenie profili osobowościowych lub śledzenie przemieszczania się abonentów telefonii komórkowej. Co więcej, nie przechowywano żadnych danych dotyczących poszczególnych zdarzeń komunikacyjnych. Poziom ingerencji należy zatem wyraźnie odróżnić od poprzednich spraw Trybunału, które dotyczyły na przykład „pomiaru” (*metering*) (zob. *Malone i Copland*, obie sprawy cyt. powyżej), geolokalizacji (zob. *Uzun i Ben Faiza*, obie sprawy cyt. powyżej) lub przechowywania danych dotyczących zdrowia lub innych danych wrażliwych (zob. na przykład *S. i Marper*, cyt. powyżej, oraz *M.M. przeciwko Zjednoczonemu Królestwu*, nr 24029/07, 13 listopada 2012 r.). Ponadto, niniejszą sprawę należy odróżnić od spraw, w których rejestracja w określonej bazie danych prowadziła do częstych kontroli lub do dalszego gromadzenia informacji prywatnych (zob. *Dimitrov-Kazakov przeciwko Bułgarii*, nr 11379/03, 10 lutego 2011 r., oraz *Shimovolos przeciwko Rosji*, nr 30194/09, 21 czerwca 2011 r.).

40. Wreszcie, w zakresie, w jakim skarżący twierdzili, że ingerencja była poważna, ponieważ art. 111 ustawy telekomunikacyjnej tworzył rejestr wszystkich użytkowników mobilnych kart SIM i w tym sensie była porównywalna z zatrzymywaniem danych będącym przedmiotem spraw *Digital Rights Ireland i Seitlinger i Inni* oraz *Tele2 Sverige i Tom Watson i Inni* (zob. paragrafy 51-52 powyżej), Trybunał zauważa, że dyrektywa będąca przedmiotem tych spraw dotyczyła danych o ruchu i lokalizacji

zarówno osób prawnych, jak i osób fizycznych oraz powiązanych danych koniecznych do identyfikacji abonenta lub zarejestrowanego użytkownika.

41. Rzeczywiście, dane będące przedmiotem niniejszej sprawy wykazują większe podobieństwo do danych będących przedmiotem innego odesłania prejudycjalnego, *Ministerio fiscal* (zob. paragraf 54 powyżej). Jak stwierdził TSUE w tamtej sprawie, przedmiotowe dane „nie pozwalają na poznanie daty, godziny, czasu trwania i odbiorców połączeń dokonywanych za pomocą danej karty lub kart SIM, ani miejsc, w których te połączenia się odbyły, lub częstotliwości tych połączeń z konkretnymi osobami w danym okresie. Dane te nie pozwalają zatem na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego osób, których dane dotyczą”. TSUE stwierdził zatem, że dostęp do przedmiotowych danych nie może być określony jako poważna ingerencja w prawa podstawowe osób, których dane dotyczą (zob. paragraf 55 powyżej).

42. Podsumowując, Trybunał stwierdził, że ingerencja, choć nie była trywialna, miała raczej ograniczony charakter.

43. Jeśli chodzi o zabezpieczenia, Trybunał zauważył, że skarżący nie zarzucili, że przedmiotowe przechowywanie danych było obarczone jakimikolwiek technicznymi zagrożeniami. Ponadto czas przechowywania jest ograniczony do upływu roku kalendarzowego następującego po roku, w którym zakończył się stosunek umowny (art. 111 ust. 4 ustawy telekomunikacyjnej - zob. paragraf 27 powyżej). Taki okres przechowywania nie wydaje się niewłaściwy, biorąc pod uwagę, że dochodzenia w sprawie przestępstw mogą trwać pewien czas i wykraczać poza koniec stosunku umownego. Ponadto przechowywane dane wydają się być ograniczone do informacji koniecznych do jednoznacznej identyfikacji danego abonenta.

44. Trybunał dalej zauważył, że chociaż skarżący zarzucili jedynie przechowywanie ich danych osobowych na podstawie art. 111 ustawy telekomunikacyjnej, obie strony zaakceptowały, że przechowywanie danych musiało być oceniane w powiązaniu z art. 112 i 113 tej ustawy. Rząd twierdził, że te artykuły, w powiązaniu z innymi przepisami szczególnymi dotyczącymi wyszukiwania danych, ograniczały dostęp do danych i ich wykorzystanie oraz stanowiły skuteczne zabezpieczenia przed nadużyciami. Skarżący jednak twierdzili, że każde kolejne działanie dochodzeniowe dotycząca zachowania danej osoby - związane z łącznością ruchomą - opierało się na informacjach przechowywanych na podstawie art. 111 ustawy telekomunikacyjnej, a zatem przy ocenie proporcjonalności przepisu w odniesieniu do przechowywania danych należało uwzględnić możliwości późniejszego wykorzystania ich danych osobowych. Trybunał zgadza się ze stronami, że w niniejszej sprawie nie może rozważyć proporcjonalności ingerencji bez dokładnej oceny przyszłego możliwego dostępu do przechowywanych danych i ich wykorzystania. Dlatego też uznaje za istotne rozważenie podstawy prawnej wniosków o udzielenie informacji

oraz dostępnych zabezpieczeń (zob. *mutatis mutandis*, *S. i Marper*, cyt. powyżej, §§ 67 i 103, z dalszymi odniesieniami).

45. W odniesieniu do art. 112 ustawy telekomunikacyjnej Trybunał zgadza się z Federalnym Trybunałem Konstytucyjnym (zob. § 156 wyroku Federalnego Trybunału Konstytucyjnego przywołanego w paragrafie 18 powyżej), że przepis ten bardzo uprościł wyszukiwanie danych dla władz. Scentralizowana i zautomatyzowana procedura pozwala na formę dostępu, która w dużej mierze eliminuje praktyczne trudności związane z gromadzeniem danych i bezzwłocznie udostępnia dane organom w dowolnym momencie. Jednak fakt, że organy, które mogą wnioskować o dostęp są wymienione w art. 112 ustawy telekomunikacyjnej, jest czynnikiem ograniczającym. Mimo że lista ta wydaje się obszerna, wszystkie wymienione w niej organy zajmują się egzekwowaniem prawa lub ochroną bezpieczeństwa narodowego.

46. Jeżeli chodzi o art. 113 ustawy telekomunikacyjnej, Trybunał zauważył przede wszystkim, że wyszukiwanie informacji nie jest uproszczone w takim samym stopniu jak w przypadku art. 112, ponieważ organy muszą złożyć pisemny wniosek o poszukiwane informacje. Kolejną różnicą między art. 112 i 113 ustawy telekomunikacyjnej jest to, że organy uprawnione do wnioskowania o dostęp na podstawie tego drugiego przepisu są określone w odniesieniu do wykonywanych przez nie zadań, ale nie są wyraźnie wymienione. Chociaż Trybunał uważa, że taki opis według zadań jest mniej konkretny i bardziej otwarty na interpretację, to jednak brzmienie przepisu jest wystarczająco szczegółowe, aby jasno przewidzieć, które organy są uprawnione do wystąpienia z wnioskiem o informacje. W tym zakresie Trybunał zauważa również, że Federalny Trybunał Konstytucyjny uznał, iż ograniczone zadania służb wywiadowczych uzasadniają ich szerokie uprawnienia do żądania informacji z wyprzedzeniem (zob. § 177 wyroku Federalnego Trybunału Konstytucyjnego przywołanego w paragrafie 21 powyżej).

47. W odniesieniu do obu przepisów Trybunał zauważył, że przechowywane dane są dodatkowo chronione przed nadmiernymi lub niewłaściwymi wnioskami o informacje przez fakt, że organ wnioskujący potrzebuje dodatkowej podstawy prawnej, aby wyszukiwać dane. Jak wyjaśnił Federalny Trybunał Konstytucyjny poprzez analogię „podwójnych drzwi” (zob. § 123 wyroku Federalnego Trybunału Konstytucyjnego przywołanego w paragrafie 14 powyżej), art. 112 i 113 ustawy telekomunikacyjnej pozwalają na udostępnienie danych jedynie Federalnej Agencji ds. Sieci lub odpowiedniemu dostawcy usług. Wymagany jest jednak kolejny przepis prawny, który umożliwiłby określonym organom wystąpienie z wnioskiem o informacje. Ponadto, wyszukiwanie danych jest ograniczone do danych koniecznych, a ten wymóg konieczności jest zabezpieczony ogólnym zobowiązaniem odpowiednich organów wyszukujących informacje do usunięcia bez zbędnej zwłoki wszelkich

danych, które nie są im potrzebne. Federalny Trybunał Konstytucyjny zwrócił uwagę, że w kontekście ścigania przestępstw wymóg „konieczności” oznaczał, iż musiało istnieć przynajmniej wstępne podejrzenie (zob. § 177 wyroku Federalnego Trybunału Konstytucyjnego przywołanego w paragrafie 21 powyżej). Trybunał przyznaje, że istnieją wystarczające ograniczenia uprawnień do żądania informacji oraz że wymóg „konieczności” jest nie tylko nierozdzielnie związany z konkretnymi przepisami prawnymi będącymi przedmiotem niniejszej skargi, ale także z niemieckim i europejskim prawem w zakresie ochrony danych.

48. Biorąc pod uwagę te elementy, Trybunał może zaakceptować wniosek Federalnego Trybunału Konstytucyjnego, że progi przewidziane w art. 113 ustawy telekomunikacyjnej były nadal dopuszczalne w świetle prawa konstytucyjnego, uwzględniając również fakt, że obowiązek złożenia pisemnego wniosku o informacje prawdopodobnie zachęcał organ do uzyskiwania informacji tylko wtedy, gdy były one wystarczająco potrzebne (zob. § 178 wyroku Federalnego Trybunału Konstytucyjnego przywołanego w paragrafie 21 powyżej). W związku z tym Trybunał zauważa również, że w praktyce ręczne wyszukiwanie informacji rzeczywiście wydawało się być dokonywane w ograniczonej liczbie przypadków, w porównaniu ze zautomatyzowanymi wnioskami na mocy art. 112 ustawy telekomunikacyjnej (zob. paragraf 13 powyżej).

49. Na koniec, Trybunał rozważy dostępne możliwości kontroli i nadzoru nad wnioskami o informacje na podstawie art. 112 i 113 ustawy telekomunikacyjnej. W sprawie *Klass i Inni przeciwko Niemcom* (6 września 1978 r., § 55, Seria A nr 28) Trybunał uznał, że kontrola ingerencji w prawo do poszanowania życia prywatnego na podstawie art. 8 Konwencji - w tym przypadku ingerencji, które przybrały formę tajnych środków inwigilacji - może mieć miejsce na trzech różnych etapach: gdy ingerencja została zarządzona po raz pierwszy, w trakcie jej wykonywania lub po jej zakończeniu. W przypadkach, gdy kontrola została przeprowadzona bez wiedzy jednostki podczas dwóch pierwszych etapów, istotne było, aby ustanowione procedury same zapewniały odpowiednie i równoważne gwarancje zabezpieczające prawa jednostki. W bardziej ogólnym tonie Trybunał stwierdził (ibid.):

„...wartości społeczeństwa demokratycznego muszą być jak najwierniej przestrzegane w procedurach nadzorczych, jeśli nie mają zostać przekroczone granice konieczności, w rozumieniu art. 8 ust. 2. Jedną z podstawowych zasad społeczeństwa demokratycznego jest zasada rządów prawa, do której wyraźnie nawiązuje Preambuła Konwencji ... Rządy prawa oznaczają między innymi, że ingerencja organów wykonawczych w prawa jednostki powinna podlegać skutecznej kontroli, którą w normalnych warunkach powinno zapewnić sądownictwo, przynajmniej w ostateczności, zważywszy że kontrola sądowa daje najlepsze gwarancje niezależności, bezstronności i właściwej procedury.”

50. Następnie powołał się na te zasady, w szczególności na możliwości skutecznej kontroli i przeglądu, dotyczące różnych ingerencji w prawo do poszanowania życia prywatnego na podstawie art. 8 Konwencji (zob., na przykład: przechowywanie wrażliwych danych osobowych w aktach bezpieczeństwa, *Rotaru przeciwko Rumunii* [WI], nr 28341/95, § 59, ETPC 2000V; zajęcie dokumentów bankowych, *M.N. i inni*, cyt. powyżej, §§ 73 i 78; decyzja o uchyleniu przywileju pani adwokat wobec ujawnienia jej wyciągów bankowych w postępowaniu karnym, *Brito Ferrinho Bexiga Villa-Nova przeciwko Portugalii*, nr 69436/10, § 55, 1 grudnia 2015; podsłuch telefoniczny, *Lambert przeciwko Francji*, 24 sierpnia 1998 r., § 31, *Reports of Judgments and Decisions* 1998-V; system tajnego nadzoru nad łącznością ruchomą, *Roman Zakharov*, cyt. powyżej, § 233; oraz strategiczne monitorowanie łączności, *Weber i Saravia przeciwko Niemcom* (dec.), nr 54934/00, § 117, ETPC 2006-XI). Trybunał zauważa jednak, że wszystkie te sprawy dotyczyły zindywidualizowanych oraz poważniejszych i bardziej inwazyjnych ingerencji w prawo do poszanowania życia prywatnego, które nie mogą być porównywane z kwestią dostępu do danych w niniejszej sprawie. Podsumowując, Trybunał uznał, że poziom kontroli i nadzoru należy uznać za istotny, ale nie decydujący, element oceny proporcjonalności gromadzenia i przechowywania tak ograniczonego zbioru danych.

51. Przechodząc do stanu faktycznego niniejszej sprawy, Trybunał zauważył, że co do zasady art. 113 ust. 2 ustawy telekomunikacyjnej wyjaśnia, że odpowiedzialność za zgodność z prawem wniosku o informacje spoczywa na agencji wyszukującej informacje, oraz że dostawcy usług telekomunikacyjnych nie mają kompetencji do kontrolowania dopuszczalności jakiegokolwiek wniosku, o ile wniosek o informacje jest składany w formie pisemnej i powołuje się na podstawę prawną. Zgodnie z art. 112 ustawy telekomunikacyjnej, Federalna Agencja ds. Sieci jest jednak właściwa do badania dopuszczalności przekazu, gdy istnieje ku temu szczególny powód.

52. Ponadto każde wyszukiwanie oraz istotne informacje dotyczące wyszukiwania (czas, dane wykorzystane w procesie, wyszukiwane dane, informacje jednoznacznie identyfikujące osobę pobierającą dane, organ wnioskujący, jego numer referencyjny, informacje jednoznacznie identyfikujące osobę wnioskującą o dane) są rejestrowane do celów nadzoru nad ochroną danych. Nadzór ten jest prowadzony przez niezależne federalne i krajowe organy ochrony danych. Te ostatnie są nie tylko właściwe do kontroli przestrzegania przepisów o ochronie danych przez wszystkie zaangażowane organy, ale może się do nich odwołać każdy, kto uważa, że jego prawa zostały naruszone poprzez gromadzenie, przetwarzanie lub wykorzystywanie jego danych osobowych przez organy publiczne.

53. W końcu Trybunał zauważył, że Federalny Trybunał Konstytucyjny orzekł, iż zadośćuczynienia prawnego za wyszukiwanie informacji można

dochodzić na zasadach ogólnych (zob. § 186 wyroku Federalnego Trybunału Konstytucyjnego przywołanego w paragrafie 22 powyżej) - w szczególności wraz z postępowaniem odwoławczym od ostatecznych decyzji organów.

54. Trybunał uważa, że możliwość nadzoru ze strony właściwych organów ochrony danych zapewnia dostępność kontroli przez niezależny organ. Ponadto, ponieważ każdy, kto uważa, że jego prawa zostały naruszone, może wnieść odwołanie, brak powiadomienia i poufność procedury wyszukiwania nie stanowi problemu w świetle Konwencji.

55. Wreszcie Trybunał przyznaje, że - ponieważ wśród państw członkowskich nie ma konsensusu co do gromadzenia i przechowywania ograniczonych informacji o abonentach (zob. paragraf 58 powyżej) - państwa członkowskie dysponują pewnym marginesem oceny przy wyborze środków służących osiągnięciu uprawnionych celów ochrony bezpieczeństwa narodowego i zwalczania przestępczości, którego Niemcy nie przekroczyły w niniejszej sprawie.

56. Mając na uwadze powyższe, Trybunał stwierdza, że przechowywanie danych osobowych skarżących przez odpowiednich dostawców ich usług na podstawie art. 111 ustawy telekomunikacyjnej (w wersji badanej przez Federalny Trybunał Konstytucyjny - zob. paragraf 64 powyżej) było proporcjonalne, a zatem "konieczne w demokratycznym społeczeństwie".

57. W związku z powyższym, nie nastąpiło naruszenie art. 8 Konwencji;

Z TYCH WZGLĘDÓW TRYBUNAŁ

1. *Uznaje* jednogłośnie skargę za dopuszczalną;
2. *Uznaje*, większością sześciu głosów do jednego, że nie doszło do naruszenia art. 8 Konwencji

Sporządzono w języku angielskim i obwieszczono pisemnie w dniu 30 stycznia 2020 r., zgodnie z Regułą 77 §§ 2 i 3 Regulaminu Trybunału.

Claudia Westerdiek
Kancierz

Yonko Grozev
Przewodniczący

Zgodnie z artykułem 45 ust. 2 Konwencji oraz Regulą 74 § 2 Regulaminu Trybunału, do niniejszego wyroku została załączona opinia odrębna sędziego Ranzoni.

Y.G.

C.W.

OPINIA ODREBNA SĄDZIEGO RANZONI

[pominięto]