



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

EUROPEJSKI TRYBUNAŁ PRAW CZŁOWIEKA
PIERWSZA SEKCJA

SPRAWA CATT przeciwko ZJEDNOCZONEMU KRÓLESTWU

(Skarga nr 43514/15)

WYROK

STRASBURG

24 stycznia 2019 r.

OSTATECZNY

24/04/2019

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

W sprawie Catt przeciwko Zjednoczonemu Królestwu,

Europejski Trybunał Praw Człowieka (Pierwsza Sekcja), zasiadając jako Izba w składzie:

Linos-Alexandre Sicilianos, *Przewodniczący*,
Aleš Pejchal,
Ksenija Turković,
Armen Harutyunyan,
Pauliine Koskelo,
Tim Eicke,
Gilberto Felici, *sędziowie*

oraz Abel Campos, *Kancierz Sekcji*,

Po obradach na posiedzeniu niejawnym w dniach 11 września i 11 grudnia 2018 r.,

Wydaje następujący wyrok, który został przyjęty w drugiej ze wskazanych wyżej dat.

POSTĘPOWANIE

1. Sprawa wywodzi się ze skargi (nr 43514/15) wniesionej w dniu 2 września 2015 r. przeciwko Zjednoczonemu Królestwu do Trybunału na podstawie art. 34 Konwencji o ochronie praw człowieka i podstawowych wolności („Konwencja”) przez obywatela brytyjskiego, pana Johna Oldroyda Catta.

2. Skarżący był reprezentowany przez pana S. Dutta z Bhatt Murphy Solicitors, adwokata z siedzibą w Londynie. Rząd Zjednoczonego Królestwa („Rząd”) był reprezentowany przez pełnomocnika, panią R. Sagoo z Foreign and Commonwealth Office.

3. W dniu 19 maja 2016 r. skarga została zakomunikowana Rządowi.

4. Komisja Równości i Praw Człowieka (Equality and Human Rights Commission) oraz organizacja pozarządowa Privacy International zostały dopuszczone do udziału w procedurze pisemnej (art. 36 ust. 2 Konwencji oraz Reguła 44 § 3 Regulaminu Trybunału).

FAKTY

[Paragrafy 5 - 71 wyroku pominięte i zastąpione tłumaczeniem poniższego streszczenia przygotowanego przez Kancelarię Europejskiego Trybunału Praw Człowieka]

Streszczenie stanu faktycznego¹:

Skarżący był aktywnym działaczem pokojowym od 1948 r.. W 2005 r. zaczął brać udział w demonstracjach organizowanych przez grupę protestującą z użyciem przemocy, które przyciągnęły znaczną liczbę policjantów. Sam skarżący nigdy nie został skazany za żadne przestępstwo, a zagrożenie, że popełni przestępstwo z użyciem przemocy, było niewielkie.

W postępowaniu krajowym skarżący starał się o usunięcie swoich danych przechowywanych w policyjnej bazie danych zwanej „Bazą danych o ekstremizmie” (*Extremism Database*). Przechowywane dane zawierały takie informacje jak jego nazwisko, adres, data urodzenia i udział w demonstracjach. Większość zapisów dotyczyła demonstracji organizowanych przez grupę protestującą z użyciem przemocy, ale inne dotyczyły obecności skarżącego na imprezach politycznych i związkowych].

PRAWO**I. ZARZUCANE NARUSZENIE ART. 8 KONWENCJI**

72. Skarżący zarzucił, że zatrzymanie jego danych przez policję stanowiło naruszenie jego prawa do prywatności, o którym mowa w art. 8 Konwencji, który brzmi następująco:

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

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

A. Dopuszczalność

73. Rząd podniósł dwa argumenty związane z dopuszczalnością.

74. Pierwszym z nich było twierdzenie, że skarżący nie jest już ofiarą w zakresie wskazanym w jego skardze, ponieważ prawie wszystkie wpisy w bazie danych, na które złożył skargę, zostały usunięte w 2012 r.

¹ Źródło: Nota informacyjna na temat orzecznictwa Trybunału nr 225, styczeń 2019 r. (*Information Note. Case-law of the European Court of Human Rights No. 225, January 2019 / Note d’information sur la jurisprudence de la Cour 225 / Janvier 2019*)

75. W związku z tym skarżący podkreślił, że jego skarga dotyczyła odmowy policji w 2010 r. usunięcia sześćdziesięciu sześciu wpisów w bazie danych, w których wymieniono go, a które były gromadzone i przechowywane począwszy od 2004 r. Fakt, że wszystkie te wpisy, z wyjątkiem sześciu, zostały usunięte w 2012 r. w kontekście procedury usuwania spowodowanej ujawnieniem tajnych informacji o pracy policji w niepowiązanych postępowaniach krajowych, nie miał znaczenia.

76. Trybunał odnotowuje, że dane skarżącego zostały po raz pierwszy zgromadzone i zatrzymane w 2005 r. (zob. paragraf 9, powyżej). Od tego czasu policja stale zatrzymywała w takiej czy innej formie jego dane osobowe w bazie danych. W związku z tym od 2005 r. miał on status ofiary z punktu widzenia Konwencji. Na taki wniosek nie ma wpływu fakt, że niektóre dane osobowe skarżącego zostały usunięte w 2012 r.

77. Drugim argumentem przedstawionym przez Rząd było to, że skarżący miał do dyspozycji szereg sądowych środków odwoławczych, z których mógł skorzystać w celu zapewnienia usunięcia swoich danych osobowych.

78. Trybunał przypomina, że zgodnie z jego utrwalonym orzecznictwem, gdy zastosowano środek odwoławczy, nie jest wymagane zastosowanie innego środka, który ma zasadniczo ten sam cel (zob. m.in. *Micallef przeciwko Malcie* [WI], nr 17056/06, § 58, ETPC 2009 oraz *Kozacioğlu przeciwko Turcji* [WI], nr 2334/03, § 40, 19 lutego 2009 r.).

79. W świetle powyższego, Trybunał stwierdza, że skarga nie jest w sposób oczywisty nieuzasadniona w rozumieniu art. 35 ust. 3 lit. a Konwencji. Trybunał zauważa przy tym, że nie jest ona niedopuszczalna z jakichkolwiek innych względów. Należy ją, zatem, uznać za dopuszczalną.

B. Przedmiot skargi

1. Stanowiska stron

80. Skarżący zarzucał, że systematyczne gromadzenie i przechowywanie informacji o nim w przeszukiwalnej bazie danych stanowiło ingerencję w jego prawo do prywatności na podstawie art. 8. Twierdził on, że ingerencja ta nie była uzasadniona, ponieważ baza danych, w której przechowywano dane, nie zapewniała wystarczających zabezpieczeń, a zatem nie była przewidziana przez ustawę. Twierdził on w szczególności, że zakres bazy danych może być dostosowywany arbitralnie przez policję; dane są zatrzymywane przez zbyt długi okres na podstawie tego, że baza danych jako całość może być użyteczna; dane podlegają zautomatyzowanemu i ręcznemu przetwarzaniu. Nie przedstawił on argumentów opartych na przepisach dotyczących ochrony danych, ale stwierdził, że zatrzymywanie danych jest nieuzasadnione, biorąc pod uwagę fakt, że zatrzymywane dane dotyczyły jego zaangażowania w prawidłową i zgodną z prawem działalność polityczną i nigdy nie były użyteczne dla jakichkolwiek funkcji policyjnych.

Zatrzymywanie takich danych może mieć skutek zniechęcający („efekt mrozący”).

81. Skarżący argumentował również, że ponieważ po wydaniu orzeczenia przez Sąd Najwyższy zostały znalezione w bazie danych zapisy, które go dotyczyły, Sąd Najwyższy wydał decyzję na podstawie niepełnych danych faktycznych. Przywołując swoje twierdzenie, że baza danych nie posiadała wystarczających zabezpieczeń, skarżący argumentował, że zapisy stanu faktycznego nie są należycie ujawniane nawet w kontekście postępowania przed Sądem Najwyższym, co wskazuje na niezgodność bazy danych z prawem. Stwierdził również, że nie istnieje rzeczywisty system nadzoru lub niezależnego przeglądu, podkreślając, że złożenie przez osoby, których dane dotyczą „wniosku o dostęp do informacji” (*subject access request*) zgodnie z ustawą o ochronie danych osobowych (DPA) będzie skuteczne tylko wtedy, gdy wszystkie istotne dane zostaną ujawnione przez policję w momencie otrzymania takiego wniosku. Skarżący twierdził również, że margines oceny, jaki należy przyznać w świetle orzeczeń sądów krajowych, jest ograniczony, biorąc pod uwagę fakt, że sądy te nie posiadały wszystkich istotnych informacji.

82. Rząd uznał, że gromadzenie i przechowywanie informacji dotyczących skarżącego stanowiło ingerencję w jego prawo do poszanowania życia prywatnego. Jednakże, opierając się na ustaleniach Sądu Najwyższego, utrzymywał, że ingerencja ta była bardzo ograniczona.

83. Opierał się również na ustaleniach Sądu Najwyższego, że ingerencja ta była przewidziana przez ustawę, podlegając ustawie o ochronie danych osobowych z 1998 r. oraz ustawowemu kodeksowi praktyki i wytycznych (*Code of Practice and Guidance*).

84. Jeśli chodzi o konieczność przechowywania informacji dotyczących skarżącego, Rząd podkreślił, że różnice zdań między Sądem Apelacyjnym a Sądem Najwyższym odzwierciedlają opinie obu sądów na temat dowodów. Odnosząc się do szerokiego zakresu kontroli sądowej w tej kwestii na szczeblu krajowym, utrzymywał on, że to, czy konieczne jest zatrzymanie danych skarżącego, mieści się w granicach marginesu oceny państwa.

85. W odniesieniu do ujawnienia dodatkowych raportów dotyczących skarżącego po zakończeniu postępowania krajowego Rząd stwierdził, że nie mają one żadnego szczególnego wpływu na treść wyroków krajowych i że skarżący powinien skorzystać z krajowych środków odwoławczych w celu wniesienia skargi dotyczącej tych ujawnień, na przykład w drodze kontroli sądowej.

2. Oświadczenia interwenientów ubocznych

a) Komisja Równości i Praw Człowieka

86. Komisja Równości i Praw Człowieka (Equality and Human Rights Commission, EHRC) przedłożyła uwagi dotyczące bazy danych

o ekstremizmie (*Extremism Database*), którą określiła jako skomputeryzowaną i przeszukiwalną policyjną bazę danych, gdzie przechowywane są duże ilości danych wywiadowczych na temat legalnych protestów publicznych i osób biorących w nich udział. Według EHRC, baza danych nie została utworzona na mocy żadnego aktu ustawowego, nie ma żadnych podstaw prawnych i żadna opublikowana polityka nie odnosi się do jej utworzenia, celów lub funkcji.

87. W interwencji przywołano odpowiednie normy i wytyczne określone w różnych instrumentach międzynarodowych, w tym w art. 17 Międzynarodowego paktu praw obywatelskich i politycznych oraz w zaleceniu R (87) 15 Komitetu Ministrów Rady Europy dotyczącym wykorzystania danych osobowych w sektorze policji. Opierając się na orzecznictwie tego Trybunału oraz Trybunału Sprawiedliwości Unii Europejskiej, Komisja dalej określiła, co uważa za podstawowe minimalne zasady wymagane do spełnienia wymogu, aby reżim prawny był „przewidziany przez ustawę” w kontekście policyjnej bazy danych będącej przedmiotem niniejszej sprawy. Są to następujące zasady:

- (i) nadanie uprawnień policji musi być publikowane i publicznie dostępne;
- (ii) wymagane są jasne i publicznie dostępne zabezpieczenia w celu zagwarantowania, by ingerencja nie nastąpiła w sposób arbitralny, niewłaściwy lub niepotrzebny;
- (iii) muszą istnieć jasne i dostępne kryteria umożliwiające osobom fizycznym, których dane osobowe są przechowywane, zapewnienie ich usunięcia, w tym w drodze niezależnej kontroli;
- (iv) należy usuwać informacje dotyczące osób, których nie podejrzewa się o działalność przestępczą.

88. Następnie EHRC stwierdziła brak minimalnych zabezpieczeń bazy danych o ekstremizmie. Podkreśliła również niebezpieczeństwo „efektu mrożącego” dla uprawnionych protestów politycznych, w przypadku gdy baza danych o ekstremizmie zawiera informacje o działalności politycznej.

b) Privacy International

89. Privacy International jest organizacją pozarządową z siedzibą w Zjednoczonym Królestwie, która zajmuje się bezprawnym wykorzystywaniem nadzoru (*surveillance*).

90. Privacy International skrytykowała dokonaną przez Sąd Najwyższy kwalifikację ingerencji w prawo skarżącego do prywatności jako drobną, ponieważ dotyczy ona działań, które miały miejsce publicznie, podkreślając, że gromadzenie takich informacji powinno być postrzegane w tym kontekście. Privacy International argumentowała, że wraz z szybkim rozwojem technologicznym podejście to umożliwiłoby monitorowanie dużych ilości informacji, które są w pewnym stopniu publiczne, takich jak informacje z mediów społecznościowych, technologia rozpoznawania

twarzy, kamery noszone na ciele, CCTV i technologia automatycznego rozpoznawania tablic rejestracyjnych. Skrytykowała brak ustawodawstwa regulującego gromadzenie i wykorzystywanie danych uzyskanych z takich źródeł.

91. Privacy International stwierdziła, że zatrzymywanie takich danych jest naruszeniem prawa do prywatności, a także prawa do wolności wyrażania opinii, podkreślając ponownie, że takie naruszenie nie może być uznane za drobne.

3. Ocena Trybunału

a) Ingerencja

92. W świetle wniosków Sądu Najwyższego Rząd przyznał, że gromadzenie i przechowywanie danych osobowych skarżącego naruszało jego prawa wynikające z art. 8. Twierdził on jednak, że naruszenie praw skarżącego było ograniczone.

93. Trybunał przypomina, że w jego orzecznictwie powszechnie uznaje się, że samo przechowywanie informacji stanowi ingerencję w prawo skarżących do poszanowania życia prywatnego, zagwarantowane w art. 8 ust. 1 Konwencji (zob. *S. i Marper*, cyt. powyżej, § 67 i *Segerstedt-Wiberg i inni przeciwko Szwecji*, nr 62332/00, § 73, ETPC 2006-VII z dalszymi odniesieniami). Trybunał uważa, że do kwestii rzekomego „ograniczonego” charakteru ingerencji w prawa skarżącego należy raczej podejść w kontekście tego, czy ingerencja ta była konieczna w demokratycznym społeczeństwie (zob. paragrafy 109-128, poniżej).

b) Uzasadnienie

(i) Przewidziana przez ustawę

94. Jak przypomniał Trybunał, wyrażenie „przewidziany przez ustawą” nie tylko wymaga, aby zaskarżony środek miał pewne podstawy w prawie krajowym, ale także odnosi się do jakości przedmiotowego prawa, wymagając, aby było ono dostępne dla zainteresowanej osoby i przewidywalne co do jego skutków. Aby prawo krajowe spełniało te wymogi, musi ono zapewniać odpowiednią ochronę prawną przed arbitralnością i w związku z tym wskazywać dostatecznie jasno zakres i swobodę decyzyjną przyznaną właściwym organom oraz sposób jego wykonywania (zob. m.in. *M.M. przeciwko Zjednoczonemu Królestwu*, nr 24029/07, § 193, 13 listopada 2012 z dalszymi odniesieniami).

95. Trybunał zauważył również, że istnieją różne kluczowe etapy, na których mogą pojawić się kwestie ochrony danych na mocy art. 8 Konwencji, w tym podczas gromadzenia, przechowywania, wykorzystywania i przekazywania danych (*M.M.*, cyt. powyżej, § 195).

(α) Gromadzenie danych

96. W odniesieniu do kwestii gromadzenia danych Trybunał odnotowuje, że w niniejszej sprawie gromadzenie danych odbywało się na podstawie ogólnych uprawnień policyjnych w common law, w odniesieniu do roboczej definicji „ekstremizmu krajowego”. Definicja ta różniła się w zależności od organów policyjnych, a jej niejednoznaczność była krytykowana przez Inspektorat Policji Jej Królewskiej Mości (*Her Majesty's Inspectorate of Constabulary*, „HMIC”, zob. paragraf 52 powyżej).

97. W świetle ogólnego charakteru uprawnień policji oraz różnorodności definicji terminu „ekstremizm krajowy” Trybunał uważa, że istniała znaczna niejednoznaczność co do kryteriów stosowanych przez policję przy gromadzeniu przedmiotowych danych. Trybunał zauważa, że – jak się wydaje – być może w związku z tym przedmiotowa baza danych została zgromadzona w sposób nieco doraźny. Dlatego Trybunał zgadza się ze skarżącym, że na podstawie dostępnych informacji trudno jest określić dokładny zakres i treść gromadzonych i opracowywanych danych w celu utworzenia bazy danych.

98. Jednak Rząd argumentował, że utworzenie bazy danych nie musi być ustawowo umocowane. Trybunał uważa, że twierdzenie to jest poparte zasadą 3.1. rezolucji Komitetu Ministrów (74) 29 w sprawie ochrony prywatności osób fizycznych wobec elektronicznych banków danych w sektorze publicznym (zob. paragraf 61 powyżej), która stanowi, że powstanie takich banków danych musi być przewidziane w ustawie lub w specjalnym rozporządzeniu albo podane do wiadomości publicznej w oświadczeniu lub dokumencie, zgodnie z systemem prawnym każdego państwa członkowskiego. W związku z tym Trybunał zauważa, że „zarządzanie” danymi było regulowane ustawodawstwem i kodeksem postępowania (zob. paragrafy 37-40 i paragraf 99), podczas gdy ogólne uprawnienia policji, które pozwalały na gromadzenie danych, były przewidziane w common law. Na poparcie swojego wniosku, że gromadzenie danych skarżącego było możliwe do przewidzenia, Sąd Najwyższy powołał się na sprawozdanie HMIC z 2003 r. (zob. § 28 jego wyroku) oraz na równoczesne doniesienia prasowe. Trybunał zauważa, że istnienie konkretnej bazy danych zostało wyraźnie uznane dopiero w postępowaniu krajowym w tej sprawie, chociaż przyznaje, że na podstawie publicznie dostępnych informacji można było wywnioskować, że policja prawdopodobnie prowadziła taką bazę danych.

99. Obawy budzi fakt, że gromadzenie danych do celów tej bazy danych nie miało jaśniejszej i bardziej spójnej podstawy prawnej. Ramy regulujące gromadzenie danych dotyczących skarżącego nie mogą być jednak postrzegane w oderwaniu od przepisów regulujących zatrzymywanie i wykorzystywanie danych osobowych skarżącego. W związku z tym, zanim dojdzie do rozstrzygnięcia w tym zakresie, Trybunał zamierza zbadać przepisy, które nakładają pewne środki ochrony prawnej przed arbitralnością.

(β) Zatrzymywanie i wykorzystywanie danych

100. Trybunał zbadał ostatnio przepisy regulujące zatrzymywanie danych w niniejszej sprawie w cytowanym powyżej wyroku w sprawie *M.M.* Przepisy te to ustawa o ochronie danych osobowych (*Data Protection Act*) oraz Kodeks postępowania w zakresie zarządzania informacjami policyjnymi (*Code of Practice on the Management of Police Information*, „MoPI”) z 2005 r. W niniejszej sprawie przepisy dotyczące zatrzymywania danych stwierdzają, że istnieje domniemanie przemawiające za zatrzymywaniem danych, jeżeli dane nie są nadmierne, są niezbędne dla celów policyjnych i są aktualne. Po początkowej decyzji o zatrzymaniu dane muszą być zatrzymane przez okres co najmniej sześciu lat. Po upływie tego okresu należy je poddać przeglądowi i mogą zostać usunięte. Nie ma ustalonego terminu, w którym należy dokonać przeglądu danych lub w którym należy je usunąć. Policja zachowuje ogólną swobodę decydowania o zatrzymywaniu danych, jeżeli jest to konieczne.

101. W cytowanym powyżej wyroku w sprawie *M.M.* Trybunał stwierdził naruszenie art. 8 na podstawie tego, że zatrzymywanie i ujawnianie danych osobowych nie było przewidziane przez ustawę. Zauważył, że nieselektywne i nieograniczone gromadzenie danych z rejestrów karnych najprawdopodobniej nie będzie zgodne z wymogami art. 8 przy braku jasnych i szczegółowych przepisów ustawowych wyjaśniających obowiązujące zabezpieczenia i określających zasady regulujące, między innymi, okoliczności, w jakich dane mogą być gromadzone, czas ich przechowywania, sposób ich wykorzystania oraz okoliczności, w jakich mogą zostać zniszczone. Zauważył również brak jakiegokolwiek mechanizmu niezależnej kontroli decyzji o zatrzymaniu lub ujawnieniu danych (zob. *M.M.*, cyt. powyżej, §§ 199-206).

102. Jednak o ile przepisy dotyczące zatrzymywania danych w obecnej sprawie są w pewnym stopniu podobne do przepisów dotyczących sprawy *M.M.*, inne elementy nie są takie same.

103. W pierwszej kolejności Trybunał zauważa, że sprawa *M.M.* dotyczyła zatrzymywania danych z rejestrów karnych, które Trybunał określił jako nie tylko osobowe, ale także wrażliwe, z „potencjalnie druzgocącymi skutkami” w przypadku ich ujawnienia. Co więcej, skarga w sprawie *M.M.* nie dotyczyła gromadzenia danych przez policyjne służby wywiadowcze, ale koncentrowała się na reżimie ujawniania danych z rejestrów karnych, a Trybunał skrytykował brak ustawowych ram regulujących (w niektórych przypadkach obowiązkowe) przekazywanie takich danych przez policję potencjalnym pracodawcom w Irlandii Północnej w tym czasie (zob. *M.M.*, cyt. powyżej, § 203).

104. W tym kontekście Trybunał zauważa również, że w przeciwieństwie do skarżącego w sprawie *M.M.*, skarżący w niniejszej sprawie miał możliwość złożenia wniosku o kontrolę i usunięcie swoich danych, z której skorzystał (zob. a contrario *M.M.*, cyt. powyżej, § 206).

(γ) Wniosek

105. Trybunał wyraża obawy związane z niejednoznacznością podstawy prawnej gromadzenia danych osobowych skarżącego. W szczególności Trybunał zwraca uwagę na luźno zdefiniowane pojęcie „ekstremizmu krajowego” oraz na fakt, że dane skarżącego mogą być zatrzymywane potencjalnie na czas nieokreślony. Jednak zatrzymane dane nie zostałyby ujawnione stronom trzecim; a skarżący miał możliwość złożenia wniosku o usunięcie swoich danych.

106. W związku z tym Trybunał przypomina, że kwestia, czy gromadzenie, zatrzymywanie i wykorzystywanie danych osobowych skarżącego było przewidziane przez ustawę prawem, jest ściśle związana z szerszą kwestią, czy ingerencja ta była konieczna w demokratycznym społeczeństwie (zob. *S. i Marper*, cyt. powyżej, § 99 ETPC 2008).

107. W związku z tym, w świetle analizy przedstawionej w paragrafach 109-128 poniżej, Trybunał nie uważa za konieczne decydowanie, czy ingerencja była „przewidziana przez ustawę” w rozumieniu art. 8 ust. 2 Konwencji.

(ii) Uprawniony cel

108. Nie było znaczącego sporu co do tego, czy utworzenie i utrzymanie bazy danych przez policję dąży do osiągnięcia uprawnionego celu. Trybunał również uważa, że policja dąży do takiego celu, a jest nim ochrona porządku i zapobieganie przestępstwom oraz ochrona praw i wolności innych osób.

(iii) Konieczna w demokratycznym społeczeństwie.

109. Trybunał wielokrotnie określał elementy, które należy wziąć pod uwagę przy rozważaniu, czy ingerencja w prawa skarżącego wynikające z art. 8 była konieczna, a zatem uzasadniona. W społeczeństwie demokratycznym będzie ona konieczna, jeżeli będzie odpowiadać na „nagłą potrzebę społeczną”, jeżeli będzie proporcjonalna do uprawnionego celu, do którego zmierza, i jeżeli powody podane przez władze krajowe w celu jej uzasadnienia są „istotne i wystarczające”. W ocenie tej należy pozostawić właściwym organom krajowym margines oceny (zob. *S. i Marper*, cyt. powyżej, § 101-102).

110. Zajmując się najpierw tym ostatnim elementem, Trybunał zauważa argument Rządu, iż sądy krajowe dokładnie zbadały te kwestie w świetle art. 8. Sądy te różniły się w swoich wnioskach, ale wskazywało to na to, że chodziło o punkt, w którym prawidłowe stosowanie zasad na podstawie art. 8 mogło jednak przynieść różny wynik. Odnosząc się do szerokiego zakresu kontroli sądowej na szczeblu krajowym, Rząd utrzymywał, że to, czy konieczne jest zatrzymanie danych skarżącego, mieści się w ramach marginesu oceny państwa, a zatem decyzja nie należy do tego Trybunału.

111. W tym względzie Trybunał przypomina, że w sprawach z art. 8 generalnie rozumie margines oceny jako oznaczający, że gdy niezależne i bezstronne sądy krajowe dokładnie zbadały fakty, stosując odpowiednie standardy praw człowieka zgodnie z Konwencją i związanym z nią orzecznictwem i odpowiednio wyważyły osobisty interes skarżącego w stosunku do bardziej ogólnego interesu publicznego w sprawie, nie jest jego zadaniem zastąpienie oceny właściwych organów krajowych własną oceną merytoryczną (w tym w szczególności własną oceną okoliczności faktycznych dotyczących proporcjonalności), chyba że zostanie wykazane, że istnieją ku temu istotne powody (zob. *McDonald przeciwko Zjednoczonemu Królestwu*, nr 4241/12, § 57, 20 maja 2014 r.).

112. Trybunał uważa jednak, że w niniejszej sprawie istnieją ku temu powody. Po pierwsze, uważa za istotne, że dane osobowe ujawniające opinie polityczne należą do specjalnych kategorii danych wrażliwych, które wymagają zwiększonego poziomu ochrony (zob. paragrafy 58-60 i 67-70 powyżej oraz *S. i Marper*, cyt. powyżej, § 76). Zauważa, że na szczeblu krajowym ten element skargi został określony jako dotyczący przepisów o ochronie danych i nie stanowił przedmiotu szczególnej uwagi podczas postępowania sądowego. Stwierdziwszy, że zatrzymanie danych skarżącego nie było uzasadnione na podstawie art. 8, Sąd Apelacyjny nie uznał, że badanie szczególnych zasad ochrony danych dodałoby cokolwiek do ich analizy (zob. § 65). Skarżący nie przedstawił konkretnych argumentów dotyczących ochrony danych przed Sądem Najwyższym, który w związku z tym odnosił się do prawa ochrony danych jedynie ogólnie w kontekście zgodności z prawem. Trybunał uważa jednak, że charakter skargi skarżącego oznaczał, że wrażliwy charakter danych, o których mowa, był głównym elementem sprawy zarówno przed sądami krajowymi, jak i przed tym Trybunałem (zob. paragraf 80 powyżej).

113. Trybunał zauważa również, że niezależnie od swojego ugruntowanego orzecznictwa (zob. paragraf 93 powyżej), sąd wyższej instancji uznał, że gromadzenie i przechowywanie danych skarżącego nie stanowi ingerencji w rozumieniu art. 8. Kwestia ta została rozstrzygnięta przez Sąd Apelacyjny i Sąd Najwyższy, które uznały, że była to ingerencja i wydały szczegółowe i obszerne wyroki odnoszące się w dużej mierze do orzecznictwa strasburskiego. Rząd podtrzymał jednak argumenty, że zatrzymywanie danych nie było systematyczne, a charakter ingerencji był ograniczony. Skarżący argumentował, że konieczne jest wydanie decydującego orzeczenia. Trybunał zgadza się, że konieczne jest pewne wyjaśnienie tych elementów.

114. Trybunał przypomina również, jak ważne jest zbadanie zgodności z zasadami określonymi w art. 8 w przypadkach, w których uprawnienia przyznane państwu są niejasne, co stwarza ryzyko arbitralności, zwłaszcza gdy dostępna technologia staje się coraz bardziej zaawansowana (zob. *Roman Zakharov przeciwko Rosji* [WI], nr 47143/06, § 229, ETPC 2015, oraz *Szabó*

i Vissy przeciwko Węgrom, nr 37138/14, § 68, 12 stycznia 2016 r.). W odróżnieniu od niniejszej sprawy, sprawy te dotyczyły niejawnego nadzoru. Trybunał uważa jednak, że powinien kierować się tym podejściem, zwłaszcza w przypadkach, w których podkreślił już obawy związane z niejednoznacznością uprawnień państwa w tej dziedzinie (zob. paragraf 105 powyżej).

115. Wreszcie, Trybunał bierze pod uwagę sposób i termin ujawnienia oraz fakt, że na temat skarżącego przechowywano więcej danych osobowych, niż ujawniono w czasie postępowania krajowego (zob. paragrafy 11 i 15-17 powyżej). Ma to wpływ na jego ocenę dostępnych zabezpieczeń (zob. paragraf 122 poniżej).

116. Dlatego też Trybunał zwraca się do innych elementów, które należy zbadać, poczynając od pytania, czy istniała „nagła potrzeba społeczna” gromadzenia i zatrzymania danych osobowych skarżącego. Przypomina przy tym, że kwestia, którą należy zbadać, nie dotyczy tego, czy istniała „nagła potrzeba społeczna”, aby policja utworzyła i prowadziła taką bazę danych. W zakresie, w jakim Trybunał bada tę kwestię z bardziej ogólnego punktu widzenia, uczynił to w swoim wniosku, że stworzenie bazy danych miało uprawniony cel (zob. paragraf 108 powyżej). Na tym etapie Trybunał bada, czy zbieranie i zatrzymanie danych osobowych skarżącego można uznać za uzasadnione na mocy Konwencji (zob. *mutatis mutandis*, *S. i Marper*, cyt. powyżej, § 106).

117. Co do tego, czy istniała nagła potrzeba zbierania danych osobowych dotyczących skarżącego, Trybunał przyjmuje, że istniała. Zgadza się z Sądem Najwyższym, że z natury gromadzenia danych przez służby wywiadowcze wynika, że policja musi najpierw zebrać te dane, zanim oceni ich wartość (zob. paragraf 27 powyżej). W tym względzie Trybunał ponownie przypomina, że dane osobowe, o których mowa, zostały uzyskane w sposób jawny.

118. Trybunał zgadza się również z sądami krajowymi, że policja odgrywała oczywistą rolę w monitorowaniu protestów *Smash EDO*, w przypadku których wiadomo było, że działania tej grupy były agresywne i potencjalnie przestępcze. Dlatego też, nawet jeśli samego skarżącego nie podejrzewano o bezpośredni udział w działalności przestępczej tej grupy, uzasadnione było, aby policja zbierała jego dane osobowe. Zdecydował się on przecież wielokrotnie i publicznie przyłączyć do działalności agresywnej grupy protestacyjnej.

119. Jeśli chodzi o to, czy istniała nagła potrzeba zatrzymania danych skarżącego, Trybunał uznaje, że nie było takiej potrzeby. Podziela on obawy sądów krajowych, że należy zachować ostrożność przed uchyleniem oceny policji o tym, jakie informacje mogą być pomocne w wykonywaniu jej zadań (zob. paragraf 22 powyżej). W tym względzie Trybunał podkreśla, że jego wniosek nie podważa faktu, iż mogła istnieć nagła potrzeba, aby policja zatrzymywała dane osobowe skarżącego przez pewien czas po ich zebraniu.

Jednakże wobec braku jakichkolwiek przepisów określających ostateczny maksymalny okres zatrzymywania takich danych, skarżący był całkowicie uzależniony od starannego stosowania bardzo elastycznych zabezpieczeń zawartych w Kodeksie postępowania w zakresie zarządzania informacjami policyjnymi („MoPI”) w celu zapewnienia proporcjonalnego zatrzymywania jego danych. W przypadku gdy państwo decyduje się na wprowadzenie takiego systemu, decydująca staje się konieczność wprowadzenia skutecznych zabezpieczeń proceduralnych (zob. odpowiednio *S.M.M. przeciwko Zjednoczonemu Królestwu*, nr 77450/12, § 84, 22 czerwca 2017 r.). Zabezpieczenia te muszą umożliwiać usunięcie wszelkich takich danych, gdy ich dalsze zatrzymywanie stanie się nieproporcjonalne.

120. W związku z tym Trybunał zauważa, że ponieważ dane osobowe skarżącego mogły być zatrzymywane potencjalnie na czas nieokreślony, jedynym terminem, którego mógł być pewien, był okres przechowywania danych przez co najmniej sześć lat, w którym to momencie zostałyby one poddane zaplanowanemu przeglądowi. W niniejszej sprawie nie jest jasne, czy te sześciolatnie lub jakiegokolwiek późniejsze przeglądy zostały przeprowadzone w jakikolwiek znaczący sposób. Z pewnością nie doprowadziły one bezpośrednio do usunięcia jakichkolwiek danych osobowych skarżącego.

121. Trybunał zauważa, że okoliczności sprawy są sprzeczne z podejściem określonym w zasadzie 4 rezolucji Komitetu Ministrów (74) 29 w sprawie ochrony prywatności osób fizycznych wobec elektronicznych banków danych w sektorze publicznym, która stanowi, że należy wydać przepisy określające maksymalne terminy, po upływie których niektóre kategorie informacji nie mogą być wykorzystywane lub przechowywane, poza niektórymi wyjątkowymi sytuacjami (zob. paragraf 62 powyżej).

122. Ponadto, chociaż skarżący mógł zażądać i zażądał ujawnienia i zniszczenia swoich danych, zabezpieczenie to wydaje się mieć ograniczony wpływ ze względu na odmowę usunięcia jego danych lub udzielenia jakiegokolwiek wyjaśnienia dotyczącego ich dalszego zatrzymywania – w tym późniejszego ujawnienia bez wyjaśnienia zatrzymywania dodatkowych danych (zob. paragrafy 11 i 15-17 powyżej). O ile Trybunałowi wiadomo, przynajmniej niektóre dane osobowe skarżącego dotyczące jego udziału w proteście bez użycia przemocy zostały zebrane ponad sześć lat temu i pozostają w krajowej bazie danych dotyczących ekstremizmu (zob. paragraf 16 powyżej), mimo że policja stwierdziła, a sądy krajowe potwierdziły, że skarżący nie został uznany za osobę stanowiącą zagrożenie dla kogokolwiek (zob. paragraf 31, powyżej).

123. Ponadto, szczególnie niepokojący w tej sprawie był brak skutecznych zabezpieczeń, ponieważ dane osobowe ujawniające opinie polityczne wymagają podwyższonego poziomu ochrony (zob. paragraf 112 powyżej). Angażowanie się w pokojowe protesty jest szczególnie chronione na mocy art. 11 Konwencji, który zawiera również specjalną ochronę dla związków

zawodowych, w których wydarzeniach skarżący brał udział (zob. paragraf 10 powyżej). W związku z tym Trybunał zauważa, że w oświadczeniu krajowego koordynatora definicja „ekstremizmu wewnętrznego” odnosi się do gromadzenia danych na temat grup i jednostek, które działają „poza procesem demokratycznym”. Dlatego wydaje się, że policja nie przestrzegała własnej definicji (choć być może płynnej (zob. paragraf 105)) przy zatrzymywaniu danych dotyczących związku skarżącego z pokojowymi wydarzeniami politycznymi: wydarzenia takie stanowią istotną część procesu demokratycznego (zob. *Gorzelik i Inni przeciwko Polsce* [WI], nr 44158/98, § 92, ETPC 2004-I). Trybunał podkreślił już niebezpieczeństwo niejednoznacznego podejścia do zakresu gromadzenia danych w niniejszej sprawie (zob. paragraf 97 powyżej). W związku z tym uważa on, że decyzje o zatrzymaniu danych osobowych skarżącego nie uwzględniały zwiększonego poziomu ochrony, jaki przysługiwał im jako danym ujawniającym poglądy polityczne, i że w tych okolicznościach zatrzymanie tych danych musiało mieć skutek zniechęcający („efekt mrożący”).

124. Ponadto, zasada 2 dotycząca gromadzenia danych zawarta w zaleceniu R (87) 15 (zob. paragraf 65 powyżej) stanowi, że gromadzenie danych dotyczących osób fizycznych wyłącznie na podstawie tego, że należą one do określonych ruchów lub organizacji, które nie są zakazane przez prawo, powinno być zakazane, chyba że jest to bezwzględnie konieczne lub służy do celów konkretnego dochodzenia (zob. odpowiednio *Segerstedt-Wiberg i Inni*, cyt. powyżej § 79). Trybunał uznaje, że nie wykazano, że zatrzymywanie danych skarżącego, w szczególności dotyczących pokojowego protestu, było bezwzględnie konieczne lub konieczne dla celów konkretnego dochodzenia.

125. Trybunał podkreśla również, że dokonuje tych ustaleń w odniesieniu do skarżącego, mając na uwadze również jego wiek, co zasada 7 zalecenia R (87) 15 określa jako szczególną okoliczność w tym kontekście (zob. paragraf 66 powyżej).

126. Rząd argumentował, że przeglądanie bazy danych i usuwanie wszystkich wpisów dotyczących skarżącego byłoby zbyt uciążliwe, ponieważ baza danych nie jest w pełni zautomatyzowana. Trybunał zauważa jednak, że wytyczne MoPI przewidują przegląd danych po sześciu latach i ich usunięcie. Chociaż nie wydaje się, aby miało to miejsce w tym przypadku, to jednak pokazuje to, że przegląd i usuwanie zapisów miało być realną możliwością. W związku z tym Trybunał przypomina również, że w 2012 r. w wyniku sprawozdania HMIC usunięto znaczną liczbę zapisów danych osobowych, co wyraźnie wskazuje, że przegląd i usuwanie zapisów są możliwe (zob. paragraf 13 powyżej). Trybunał również zauważa, że wytyczne MoPI wskazują na znaczenie zapewnienia łatwego dostępu do informacji i korzystania z nich (zob. paragraf 42 powyżej).

127. W związku z tym Trybunał nie jest przekonany, że usuwanie danych byłoby na tyle uciążliwe, aby uczynić je nieracjonalnym. Ogólnie rzecz

biorąc, Trybunał pragnie dodać, że całkowicie sprzeczne z potrzebą ochrony życia prywatnego na mocy art. 8 byłaby sytuacja, gdyby Rząd mógł stworzyć bazę danych w taki sposób, by danych w niej zawartych nie można było łatwo przeglądać lub edytować, a następnie wykorzystać to jako uzasadnienie odmowy usunięcia informacji z tej bazy.

128. Wyżej wskazane względy wystarczają, by Trybunał mógł stwierdzić, że nastąpiło naruszenie art. 8 Konwencji.

II. ZASTOSOWANIE ART. 41 KONWENCJI

129. Art. 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

130. Skarżący nie złożył wniosku o słuszne zadośćuczynienie, uznając, że stwierdzenie naruszenia będzie wystarczające. W związku z tym Trybunał uznaje, że nie ma potrzeby przyznania mu z tego tytułu żadnej kwoty.

B. Koszty i wydatki

131. Skarżący wniósł również o zwrot kosztów i wydatków poniesionych przed Trybunałem w wysokości 41 770 GBP oraz załączył szczegółową dokumentację na poparcie swojego wniosku.

132. Rząd twierdził, że kwota ta była nadmierna, w szczególności z uwagi na zbyt wysokie stawki godzinowe adwokatów, a także z uwagi na to, że ich pisma procesowe powtarzały argumenty podnoszone przed sądami krajowymi.

133. Z orzecznictwa Trybunału wynika, że skarżący jest uprawniony do zwrotu kosztów i wydatków jedynie w zakresie, w jakim zostało wykazane, że były one faktycznie poniesione, konieczne oraz uzasadnione co do wysokości. W niniejszej sprawie, mając na uwadze posiadane dokumenty oraz powyższe kryteria, Trybunał uznaje za uzasadnione przyznanie kwoty 27 000 EUR z tytułu postępowania przed Trybunałem.

C. Odsetki z tytułu zwłoki

134. Trybunał uznaje za właściwe, by odsetki z tytułu zwłoki były oparte na marginalnej stopie oprocentowania kredytu Europejskiego Banku Centralnego, do której należy dodać trzy punkty procentowe.

Z TYCH WZGLĘDÓW TRYBUNAŁ JEDNOGŁOŚNIE

1. *Uznaje* skargę za dopuszczalną;
2. *Stwierdza*, że nastąpiło naruszenie art. 8 Konwencji;
3. *Stwierdza*
 - (a) że pozwane państwo ma wypłacić skarżącemu, w ciągu trzech miesięcy od dnia, w którym wyrok stanie się ostateczny zgodnie z art. 44 ust. 2 Konwencji, następujące kwoty przeliczone na walutę pozwanego państwa według kursu obowiązującego w dniu rozliczenia:
 - (i) 27 000 EUR (dwadzieścia siedem tysięcy euro) plus wszelkie podatki, jakie mogą być nałożone na skarżącego, tytułem zwrotu kosztów i wydatków;
 - (b) że po upływie powyższego trzymiesięcznego terminu do momentu uregulowania należności, od powyższej kwoty będą naliczane zwykłe odsetki według stawki równej marginalnej (krańcowej) stopie oprocentowania kredytu Europejskiego Banku Centralnego za czas zwłoki, powiększonej o trzy punkty procentowe
4. *Oddala* pozostałą część żądania skarżącego o słuszne zadośćuczynienie.

Sporządzono w języku angielskim i obwieszczono pisemnie w dniu 24 stycznia 2019 r., zgodnie z Regulą 77 §§ 2 i 3 Regulaminu Trybunału.

Abel Campos
Kancelarz

Linos-Alexandre Sicilianos
Przewodniczący

Zgodnie z art. 45 ust. 2 Konwencji oraz Regulą 74 § 2 Regulaminu Trybunału do niniejszego wyroku załączona została opinia odrębna Sędziego Koskela, do której dołączył Sędzia Felici

L.-A.S. A.C.

ZGODNA OPINIA SĘDZIEGO KOSKELO, DO KTÓREJ
DOŁĄCZYŁ SĘDZIA FELICI

[pominięto]