



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

© Ministerstwo Spraw Zagranicznych, www.gov.pl/diplomacy

Permission to re-publish this translation has been granted by the Polish Ministry of Foreign Affairs for the sole purpose of its inclusion in the Court's database HUDOC

© Ministerstwo Spraw Zagranicznych, www.gov.pl/dyplomacja

Zezwolenie na publikację tego tłumaczenia zostało udzielone przez Ministerstwo Spraw Zagranicznych wyłącznie w celu zamieszczenia w bazie Trybunału HUDOC

EUROPEJSKI TRYBUNAŁ PRAW CZŁOWIEKA

Nota informacyjna nt. orzecznictwa Trybunału nr 236

Styczeń 2020 r.

Breyer p. Niemcom – skarga nr 50001/12

Wyrok z 30.01.2020 r. [Piąta Sekcja]

Art. 8

Art. 8 ust. 1

Poszanowanie życia prywatnego

Nałożony na dostawców usług prawny obowiązek przechowywania danych osobowych użytkowników przedpłaconych kart SIM do telefonów komórkowych i udostępnienia ich władzom na żądanie: *brak naruszenia*

Fakty – 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 – Art. 8: Zaskarżona ingerencja polegała na rzeczywistym przechowywaniu danych, a nie na ich jakimkolwiek późniejszym użyciu. Federalny Trybunał Konstytucyjny uznał

jednak, że z uwagi na możliwości ich przetwarzania i łączenia żaden z elementów danych osobowych nie jest sam w sobie nieznaczący.

Kwestia przewidywalności oraz wystarczającej szczegółowości mających zastosowanie przepisów była w niniejszej sprawie blisko powiązana z szerszym zagadnieniem, a mianowicie, czy ingerencja była konieczna w społeczeństwie demokratycznym i proporcjonalna.

W odniesieniu do tej ostatniej kwestii, z uwagi na brak konsensusu europejskiego w sprawie zbierania i przechowywania informacji na temat właścicieli przedpłaconych kart SIM, państwa członkowskie korzystają z pewnego marginesu oceny, a według Trybunału margines ten nie został przekroczony w niniejszej sprawie z następujących powodów.

Na wstępie Trybunał uznał, że z ogólnego punktu widzenia przedmiotowe przechowywanie danych stanowiło właściwą reakcję na zmiany w zachowaniach komunikacyjnych i środkach telekomunikacji:

- pre-rejestracja abonentów telefonii komórkowej znacząco uprościła i przyspieszyła dochodzenia prowadzone przez organy ścigania, mogąc się w ten sposób przyczyniać do skutecznego stosowania prawa oraz zapobiegania naruszeniom porządku lub przestępstwom;
- istnienie możliwości obchodzenia obowiązków prawnych nie może być powodem podważenia ich ogólnej użyteczności i skuteczności;
- pewien margines oceny uzasadniony był, poza brakiem konsensusu, także faktem, że w grę wchodziły względy bezpieczeństwa narodowego.

Pozostała do rozstrzygnięcia kwestia, czy ingerencja była proporcjonalna. Trybunał doszedł do odpowiedzi pozytywnej w następujący sposób:

a) *Poziom ingerencji w życie prywatne* – Inaczej niż w sprawach poprzednio badanych przez Trybunał, przedmiotowe przechowywanie danych nie dotyczyło żadnych wysoce osobistych informacji ani nie umożliwiało tworzenia profili osobowościowych lub śledzenia lokalizacji abonentów telefonii mobilnej. Ponadto nie przechowywano żadnych danych dotyczących indywidualnych wydarzeń komunikacyjnych. Choć ingerencja nie była błaha, miała raczej ograniczony charakter.

b) *Gwarancje* – W odniesieniu do samego rejestrowania i przechowywania danych, Trybunał zauważył, że:

- skarżący nie zarzucali, że przechowywanie nie było bezpieczne z technicznego punktu widzenia;
- okres trwania przechowywania był ograniczony do roku kalendarzowego po roku, w którym zakończył się stosunek umowny; nie wydaje się to nadmierne, biorąc pod uwagę, że dochodzenia w sprawie przestępstw wymagają czasu i mogą wykraczać poza okres trwania stosunku umownego;
- przechowywane dane były ograniczone do informacji niezbędnych do wyraźnego zidentyfikowania konkretnego abonenta.

Niemniej jednak należy mieć na uwadze możliwy dostęp do przechowywanych danych i ich użycie w przyszłości. W świetle poniższych kryteriów zostały w tym względzie zapewnione odpowiednie gwarancje:

i) *Uprawnienie do kierowania wniosków o informację*

Zautomatyzowane wnioski – Należy przyznać, że odpowiedni przepis przewidywał bardzo uproszczone pozyskiwanie danych przez władze. Scentralizowana i zautomatyzowana procedura zezwalała na taką formę dostępu, która w dużej mierze usuwała praktyczne trudności zbierania danych i umożliwiała udostępnianie władzom danych w każdym czasie bez zwłoki.

Jednakże organy, które mogły wnioskować o dostęp, zostały szczegółowo wymienione. Choć lista ta wydaje się szeroka, wszystkie wymienione w niej organy zajmowały się egzekwowaniem prawa lub ochroną bezpieczeństwa narodowego.

Wnioski ręczne – Należy zauważyć, że chociaż organy uprawnione do wnioskowania o dostęp na podstawie tego drugiego przepisu zostały określone poprzez odniesienie do wykonywanych przez nie zadań, nie zostały jednak wymienione wprost.

Choć opis tych organów na podstawie wykonywanych przez nie zadań był mniej konkretny i bardziej podatny na interpretację, sformułowanie przepisu było jednak wystarczająco szczegółowe, by wyraźnie określić, które organy były uprawnione do wnioskowania o informacje.

Ponadto w zakresie dotyczącym służb wywiadowczych Federalny Trybunał Konstytucyjny uznał, że ich szerokie uprawnienia do wnioskowania o informacje w celach prewencyjnych były uzasadnione, zważywszy że ich działania były ograniczone.

ii) *Cel wniosków o informacje* – Wnioskujące organy musiały mieć dodatkową podstawę prawną do uzyskania danych, co Federalny Trybunał Konstytucyjny porównał do systemu podwójnych drzwi: ustawa telekomunikacyjna zezwalała Federalnej Agencji ds. Sieci lub poszczególnym dostawcom usług jedynie na *udostępnienie* danych; aby określony organ mógł *wnioskować* o informację, musiał być do tego upoważniony przez jeszcze kolejny przepis na to zezwalający.

iii) *Zakres wniosków o informacje* – Uzyskanie danych było ograniczone do danych koniecznych (na przykład w przypadku ścigania przestępstw musiało zachodzić przynajmniej wstępne podejrzenie). Na poszczególne organy pozyskujące informacje nałożono ogólny obowiązek usunięcia bez zbędnej zwłoki wszelkich danych, których nie potrzebowały.

Ponadto wymóg „konieczności” był zawarty nie tylko w poszczególnych przepisach prawnych będących przedmiotem niniejszej skargi, ale także w niemieckim i europejskim prawie dotyczącym ochrony danych osobowych.

Choć progi dla zastosowania ręcznej procedury były niższe niż dla procedury zautomatyzowanej, obowiązek przedłożenia pisemnego wniosku o informacje mógł skłaniać władze do pozyskiwania informacji tylko wtedy, gdy była ona definitywnie konieczna. W praktyce liczba przypadków ręcznego pozyskiwania danych wydaje się znacznie mniejsza niż wniosków zautomatyzowanych.

iv) *Kontrola i nadzór nad wnioskami o informacje* – Należy przyznać, że ponieważ dostawcy telekomunikacyjni nie mieli kompetencji do sprawdzania dopuszczalności jakichkolwiek wniosków o informacje złożonych pisemnie z powołaniem się na podstawę prawną, odpowiedzialność za zgodność z prawem wniosku o informacje leżała po stronie organów je pozyskujących. Niemniej jednak:

- Federalna Agencja ds. Sieci była uprawniona do badania dopuszczalności przekazania danych, jeśli dostrzegała ku temu powody;

- każde pozyskanie danych i istotna informacja dotycząca ich pozyskania musiały być odnotowane do celów sprawowania nadzoru nad ochroną danych, który został powierzony

organom niezależnym, do których odwołać mogła się każda osoba, której dotyczyło pozyskanie danych;

- o zadośćuczynienie prawne wobec pozyskania informacji można się było ubiegać także na zasadach ogólnych – w szczególności w ramach środków zaskarżenia przeciwko ostatecznym decyzjom organów wnioskujących.

Zważywszy na te możliwości kontroli, brak powiadomienia o procedurze pozyskania danych nie rodził żadnej kwestii na podstawie Konwencji.

W każdym razie poziom kontroli i nadzoru, jakkolwiek istotny, nie może być elementem decydującym przy ocenie proporcjonalności zbierania i przechowywania tak ograniczonego zestawu danych.

Rozstrzygnięcie: brak naruszenia (sześcioma głosami do jednego)

(Zobacz także: Zestawienia tematyczne pt. [Śledzenie na masową skalę](#) oraz [Ochrona danych osobowych](#))

© Council of Europe/European Court of Human Rights
Niniejsze streszczenie przygotowane przez Kancelarię nie wiąże Trybunału.

Link do [Not informacyjnych nt. orzecznictwa](#)