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

Press Release
issued by the Registrar of the Court

ECHR 037 (2020)
30.01.2020

Requirement to collect data to identify users of pre-paid SIM cards did not violate the right to privacy

In today's **Chamber** judgment[1] in the case of Breyer v. Germany (application no. 50001/12) the European Court of Human Rights held, by **six votes to one**, that there had been:

no violation of Article 8 (right to respect for private and family life) of the European Convention on Human Rights.

The case concerned the storage of pre-paid SIM card users' data by telecommunications companies.

The Court found in particular that collecting the applicants' names and addresses as users of pre-paid SIM cards had amounted to a limited interference with their rights. The law in question had additional safeguards while people could also turn to independent data supervision bodies to review authorities' data requests and seek legal redress if necessary.

Germany had not overstepped the limits of its discretion ("margin of appreciation") in applying the law concerned and there had been no violation of the applicants' rights by the collection of the data.

Principal facts

The applicants, Patrick Breyer and Jonas Breyer, are German nationals who were born in 1977 and 1982 respectively and live in Wald-Michelbach (Germany).

In accordance with 2004 amendments to the Telecommunications Act companies had to collect and store the personal details of all their customers, including users of pre-paid SIM cards, which had not previously been required. The applicants, civil liberties activists and critics of State surveillance, were users of such cards and therefore had to register their personal details, such as their telephone numbers, date of birth, and their name and address, with their service providers.

In 2005 they lodged a constitutional complaint against various sections of the Act, including sections 111, 112 and 113. These provisions, as far as relevant in the present case, covered respectively the obligation to collect the data and for the authorities to access it, both automatically and on demand.

On 24 January 2012 the Federal Constitutional Court found that the provisions in question were compatible with the Basic Law as being proportionate and justified.

Complaints, procedure and composition of the Court

The applicants complained about the storage of their personal data as users of pre-paid SIM cards, relying on Article 8 (right to respect for private and family life, the home, and the correspondence) and Article 10 (freedom of expression).

The application was lodged with the European Court of Human Rights on 27 July 2012.

1. Under Articles 43 and 44 of the Convention, this Chamber judgment is not final. During the three-month period following its delivery, any party may request that the case be referred to the Grand Chamber of the Court. If such a request is made, a panel of five judges considers whether the case deserves further examination. In that event, the Grand Chamber will hear the case and deliver a final judgment. If the referral request is refused, the Chamber judgment will become final on that day.
Once a judgment becomes final, it is transmitted to the Committee of Ministers of the Council of Europe for supervision of its execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Judgment was given by a Chamber of seven judges, composed as follows:

Yonko **Grozev** (Bulgaria), *President*,
Angelika **Nußberger** (Germany),
Síofra **O'Leary** (Ireland),
Carlo **Ranzoni** (Liechtenstein),
Mārtiņš **Mits** (Latvia),
Lətif **Hüseynov** (Azerbaijan),
Lado **Chanturia** (Georgia),

and also Claudia **Westerdiek**, *Section Registrar.*

Decision of the Court

Article 8

The Court considered that the interference complained of was related to the storage of their personal subscriber data (telephone number, name and address, date of birth and date of contract) and the possibility for national authorities to access that data in certain defined circumstances and therefore examined the applicants' complaints under Article 8 alone.

It reiterated its case-law that protecting such data was of fundamental importance to allow people to enjoy their right to respect for private and family life, necessitating sufficient legal safeguards to prevent the use of data in a way which went against the guarantees of Article 8.

Governments had some leeway ("margin of appreciation") when pursuing the legitimate aim of protecting national security. Where there was no consensus within Council of Europe States on a particular interest or how best to protect it, then the margin of appreciation would be greater.

Existence and nature of interference

The applicants argued that the measure in question was a serious interference with their rights. Companies had to collect the data on all users, most of whom were innocent of any offence.

The Government conceded that section 111 had interfered with the applicants' right to privacy. However, the interference had been limited, had pursued legitimate aims, had limited the data to what was necessary for identification, had had a clearly defined and limited storage period, and had had sufficient safeguards against abuse.

The Court accepted that there had been an interference with the applicants' rights and examined whether it had been in line with Convention requirements of being in accordance with the law, pursuing a legitimate aim, and necessary in a democratic society.

Meeting Convention requirements for interference

On the first point, it found that the legal provisions were clear and foreseeable. Furthermore, the interference had pursued the legitimate aims of public safety, the prevention of disorder or crime and the protection of others' rights.

As to necessity, it first accepted that investigative tools had to adapt to modern means of communication when it came to fighting challenges such as organised crime and terrorism. Given the certain margin of appreciation for Member States in such circumstances, it found that the obligation to store the data was in general a suitable response to changes in communications behaviour and in the means of telecommunications.

The Court then dealt with the question of whether the interference had been proportionate and had struck a fair balance between the competing public and private interests at stake.

The Court first addressed the level of interference with the applicants' right to private life. It agreed with findings by the Federal Constitutional Court that only a limited set of data had been stored as it did not include highly personal information and communications traffic and that the level of interference in this case had to be clearly distinguished from the Court's previous cases.

It also had regard to the case-law of the Court of Justice of the European Union (CJEU) on which the applicants had relied (*Digital Rights Ireland* and *Seitlinger and Others*) and found that the data at issue in the present case bore greater resemblance to that at issue in *Ministerio Fiscal*, which had concerned police requests to access data, such as names and addresses, to identify the owners of SIM cards activated with stolen mobile telephones, where the CJEU had concluded that the access to the data could not be defined as a serious interference with the fundamental rights of the persons concerned..

The Court concluded that the interference in the present case was of a rather limited nature, albeit not trivial. It furthermore found the storage period to be not inappropriate, while the information held appeared to be limited to that necessary to identify subscribers.

Access to the data

The Court assessed the proportionality of the interference by the provisions on access to the data.

The Government argued that sections 112 and 113 in conjunction with other specific provisions for data retrieval limited access to and use of the data and constituted effective safeguards against abuse. The applicants held that the possibilities of subsequent use of their personal data by the authorities had to be taken into account.

The Court observed that the automated procedure under section 112 had very much simplified data retrieval but held that the fact that the authorities which could request access were specifically listed in section 112 and were all concerned with law enforcement or the protection of national security constituted a limiting factor. Furthermore, section 113, on the procedure for written requests for data, did not provide the precise names of bodies but gave their functions, which the Court considered was clear enough to foresee which bodies could ask for information. Both provisions provided further additional safeguards against abusive demands.

The Court lastly considered the available possibilities of review and supervision of information requests under both sections and concluded that they also provided for independent supervision by Federal and *Land* data protection authorities. In addition, the Federal Constitutional Court had ruled that legal redress against information retrieval could be sought under general rules.

Conclusions

Overall, Germany had not overstepped the certain margin of appreciation it had when choosing the means to achieve the legitimate aims of protecting national security and fighting crime.

The Court concluded that the storage of the applicants' personal data had been proportionate and "necessary in a democratic society". There had thus been no violation of the Convention.

Separate opinion

Judge Ranzoni expressed a dissenting opinion, which is annexed to the judgment.

The judgment is available only in English.

Press contacts
echrpress@echr.coe.int | tel.: +33 3 90 21 42 08

Patrick Lannin (tel: + 33 3 90 21 44 18)
Tracey Turner-Tretz (tel: + 33 3 88 41 35 30)
Denis Lambert (tel: + 33 3 90 21 41 09)
Inci Ertekin (tel: + 33 3 90 21 55 30)

The European Court of Human Rights was set up in Strasbourg by the Council of Europe Member States in 1959 to deal with alleged violations of the 1950 European Convention on Human Rights.