

# THE EUROPEAN COURT OF HUMAN RIGHTS AND THE PROTECTION OF PRIVATE LIFE AGAINST SURVEILLANCE



Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)  
Centre suisse de compétence pour les droits humains (CSDH)  
Centro svizzero di competenza per i diritti umani (CSDU)  
Swiss Centre of Expertise in Human Rights (SCHR)

In many cases, surveillance interventions breach the European Convention on Human Rights, specifically the Convention's protections of the right to privacy.

# MODERN TECHNOLOGIES AND THE ROLE OF THE EUROPEAN COURT OF HUMAN RIGHTS

**States are making increased use of new technologies, including mass surveillance technologies, in the name of national security and crime prevention.**

As early as 1989, Louis-Edmond Pettiti, a judge in the European Court of Human Rights (ECHR), warned against the impact of modern technologies. The court fulfilled its role, he said, 'by applying Article 8 [of the Convention] to its full extent and restricting states' margin of discretion, particularly in areas where the individual is becoming increasingly vulnerable due to the use of modern technologies'.

There is now a sizable body of ECHR case law on the

protection of privacy against the use of surveillance technologies. With ever-increasing technological advances, states also increasingly resort to preventive surveillance of their population in the name of security and combatting terrorism. This tendency is reflected in the growing number of complaints submitted to the ECHR concerning breaches of privacy. In the summer of 2020, almost two dozen complaints against various state laws were pending. The ECHR regularly finds that the laws at the centre of these complaints grant states extensive powers of surveillance. In many cases, the surveillance interventions permitted by these laws breach the European Convention on Human Rights, specifically the Convention's protections of the right to privacy.

# LEGAL BASIS

## SWISS FEDERAL CONSTITUTION

Article 13 of the Swiss Federal Constitution (FC) protects privacy, i.e. the right to freely conduct one's personal life as an individual, without surveillance or interference by the State. This includes private and family life, the home, postal and telecommunications, and personal data.

The Swiss Federal Court further specifies that, out of respect for privacy, communications through a telecommunications service provider must be confidential; the State is not allowed to access them and use the information gained against the persons concerned. This protection extends not only to the contents of such communications, but also to the so-called metadata of the communication process, e.g. numbers dialled, the date or the time.

## **EUROPEAN CONVENTION ON HUMAN RIGHTS**

The European Convention on Human Rights ('the Convention') guarantees the right to privacy in Article 8. While the right to self-determined conduct of one's private life is not explicitly mentioned, the ECHR interprets the right to privacy stipulated in Article 8 broadly. This article also protects private and family life, the home, postal and telecommunications and personal data.

## **SWISS FEDERAL CONSTITUTION AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS – ARE THERE ANY DIFFERENCES?**

The areas protected by Article 8 of the European Convention on Human Rights and Article 13 FC are largely comparable.

# LAUSANNE OR STRASBOURG?

Before a matter can be taken to the European Court of Human Rights in Strasbourg, recourse before all competent national courts must be exhausted. Before filing a complaint with the ECHR, the victim of a human rights violation must have brought claims in the competent Swiss courts at the various levels. The application must state in detail how the European Convention on Human Rights has been violated.

ECHR judgments often have wide-reaching impact and lead to changes in other member states. Public authorities adapt their practices and national courts refer to judgments of the court in Strasbourg.

Year	Case	ECHR judgment	Page
2020	<u>Breyer v. Germany</u>	<b>Complaint dismissed:</b> the legal obligation to collect personal data on the purchase of a prepaid SIM card does not violate Article 8 (case still pending before the Grand Chamber).	19
2018	<u>Big Brother Watch and Others v. the United Kingdom</u>	<b>Complaint partially upheld:</b> the operation of a mass surveillance system does not violate Article 8, provided the legal provisions meet certain requirements (case still pending before the Grand Chamber).	9
2017	<u>Vukota-Bojić v. Switzerland</u>	<b>Complaint upheld:</b> observation by private detectives commissioned by a state accident insurance agency violates Article 8.	21
2016	<u>Szabó and Vissy v. Hungary</u>	<b>Complaint upheld:</b> vaguely formulated surveillance measures in anti-terrorism laws violate Article 8.	11
2006	<u>Weber and Saravia v. Germany</u>	<b>Complaint dismissed:</b> the relevant law on strategic surveillance contains sufficient protective measures and therefore does not violate Article 8.	17
1998	<u>Kopp v. Switzerland</u>	<b>Complaint upheld:</b> the law in question does not restrict the scope of surveillance and official authorities' margin of discretion and therefore violates Article 8.	15

The acquisition of communications data from telecommunication providers must be authorised by a court and is permitted only for the prosecution of serious crimes.



## CASE EXAMPLE

# MASS SURVEILLANCE

**In principle, states are permitted to operate a mass surveillance regime.**

Following the revelations made by Edward Snowden on the joint surveillance programmes of the United States and the United Kingdom, 16 complainants filed three suits against the surveillance practices of the United Kingdom. These suits each concerned one of the following three parts of the British law on surveillance: mass surveillance of communications by the domestic intelligence service ('bulk interception'); national authorities acquiring communications data from communication service providers; and the exchange of intelligence with foreign governments. Each of the three suits claimed a violation of Article 8 of the Convention.

### **Mass interception of communications**

The ECHR found that the decision to operate a mass surveillance regime was within states' margin of discretion and did not in principle violate Article 8. The law on surveillance in question was, however, inadequate: for example, the law failed to stipulate any oversight over the selection of surveillance criteria, such as the search criteria for bulk interception or what material was to be analysed by which agency. In addition, it provided no protective mechanisms for preventing and taking remedial action against errors and abuses in the selection procedure for bulk interception. The United Kingdom had thereby violated Article 8.

### Acquiring retained data

Regarding the acquisition of communications data from service providers, the ECHR also found that the legal basis was not precise enough: the law obliged telecommunication providers to store data and permitted official authorities to obtain this data from the providers for the general prosecution of criminal offences. The ECHR found that this was disproportionate; the law must define this aspect more precisely and restrict the acquisition of communications data to the prosecution of serious crimes. Any acquisition of data must moreover be authorised in advance by a court or independent authority. Accordingly, this component part of the law also violated Article 8.

### Exchange with foreign governments

Regarding the exchange of intelligence with foreign governments, the ECHR found no violation of Article 8: the conditions for exchange were sufficiently specified by the law.

### Swiss law pending before the ECHR

The Swiss Federal Court, in judgment 1C\_598/2016 of 2018, ruled that the storage and acquisition of communications data was permissible and proportionate. This Swiss Federal Court judgment has been challenged and is currently pending before the ECHR.

# ANTI-TERRORISM LAWS

## **Anti-terrorism surveillance measures cannot be ordered merely on suspicion.**

In 2011, Hungary passed an anti-terrorism law that permitted secret searches of dwellings, the surveillance of private premises, the opening of postal correspondence and the monitoring of computerised communications of suspects. Máté Szabó and Beatrix Vissy lodged a complaint against the law, without knowing whether they themselves were affected by surveillance measures. They argued that such disproportionate surveillance could potentially be applied to many people, including themselves. In particular they criticised the inadequate judicial control of the anti-terrorism authorities entrusted with carrying

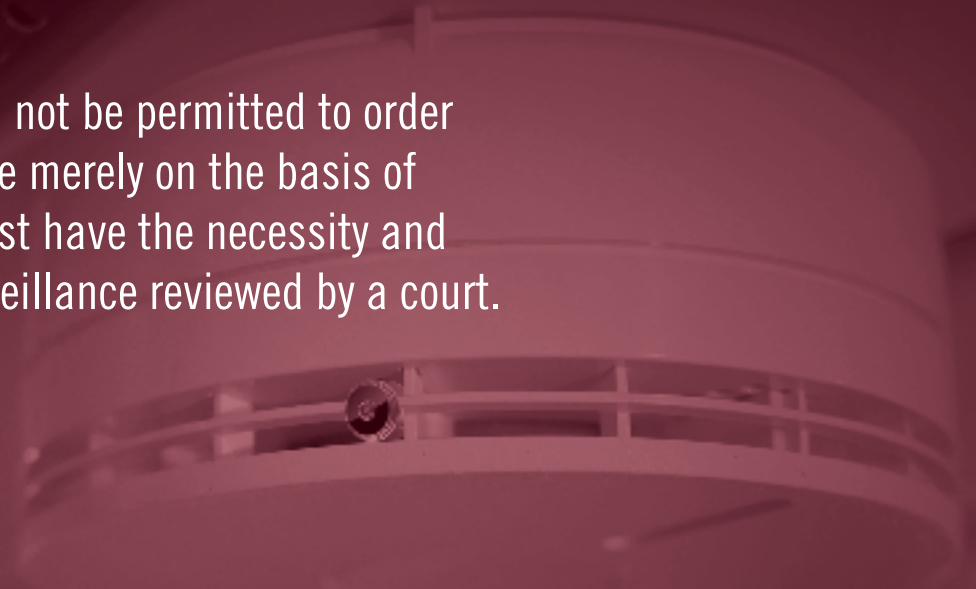
out the surveillance and the lack of any provision in the law for a prior review of the measures by a court.

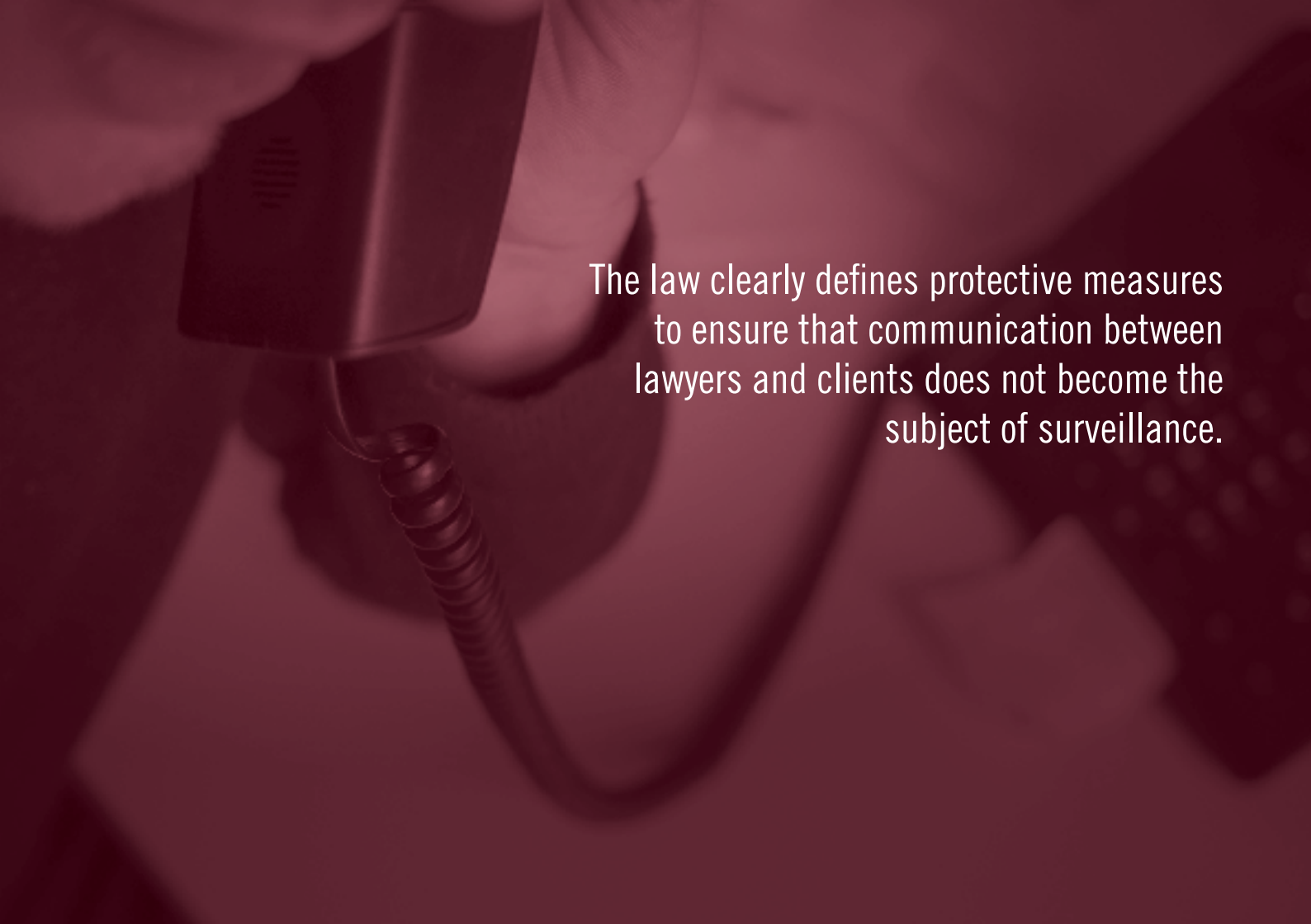
The ECHR ruled that, exceptionally for complaints against surveillance measures, an individual may claim to be a victim even if they cannot point to any concrete measures specifically affecting them. It then determined that in many respects the law was too vague: for example, it did not define sufficiently specific indications as to when surveillance measures would be ordered. Accordingly, all users of a communication system were in fact directly affected by the law in question, including the complainants. In addition, the law did not provide sufficient protection against the

abuse of surveillance measures. And finally, it was found that the competent authority should not be permitted to order surveillance merely on the basis of an 'individual suspicion' without a prior review of the necessity and proportionality of such an order by a court.

The ECHR therefore found the surveillance measures set out in the law to be a violation of Article 8.

Official authorities should not be permitted to order anti-terrorism surveillance merely on the basis of a suspicion. They must first have the necessity and proportionality of the surveillance reviewed by a court.





The law clearly defines protective measures to ensure that communication between lawyers and clients does not become the subject of surveillance.

## CASE EXAMPLE


# SURVEILLANCE OF LAWYERS' OFFICES

**The monitoring of telephone conversations and other forms of surveillance is, in all cases, a significant infringement of the right to privacy.**

In 1988, the then Swiss Federal Councillor Elisabeth Kopp was suspected of passing on confidential information obtained in her official capacity to her husband, the lawyer Hans Kopp, in order to help one of his clients. The Swiss Federal Court ordered the monitoring of Mr Kopp's telephone calls. However, only calls not protected by attorney-client privilege were to be monitored, since this confidentiality must be respected absolutely. Legally, the monitoring of the telephone calls was based on the Swiss

Federal Criminal Procedure Act. After exhausting avenues of recourse in Swiss courts, Hans Kopp lodged a complaint before the ECHR, claiming the telephone surveillance breached his right to privacy under Article 8 of the Convention.

In 1998, the ECHR ruled that telephone monitoring and other forms of surveillance must be based on a precisely formulated law, specifically because surveillance technology was developing so rapidly and was associated with special risks. However, the Swiss Federal Act did not clearly set down who was to decide, or based on what criteria, whether or not a monitored telephone call was protected by attorney-client privilege. The Act should have defined the authorities' margin of discretion more clearly. The ECHR decided unanimously that there was a violation of Article 8.



Legislation must specify clear limits to surveillance measures, so as to minimise the authorities' margin of discretion and thus prevent possible abuses.



# STRATEGIC MONITORING

**Advances in technology mean that even in the case of strategic monitoring, i.e. surveillance carried out over wide areas, the data collected can provide information on individual persons.**

In 1994, the provisions of the German Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G-10 Act) were tightened. The journalist Gabriele Weber and her assistant Cesar Richard Saravia claimed in 2000 that this violated Article 8 of the Convention. They argued that, as opposed to the justified surveillance of individuals, the G-10 Act now also made possible the strategic monitoring of communications. Because of technological progress, they said, it had become

possible to identify the participants in a monitored telecommunication and hence to illegitimately collect personal data. The ECHR confirmed that such data have made it possible to glean information on individual persons.

Secret surveillance measures are always subject to the danger of an abuse of power, the court said, and there is a lack of official supervision. The ECHR notes that in a state governed by the rule of law, domestic legislation provides appropriate safeguards against arbitrary infringements of the rights provided by Article 8.

In its ruling on the suit of Weber and Saravia, the ECHR has set down explicit criteria on the provisions that legislation must contain in order to prevent abuses:

- a list of the specific criminal offences that may justify surveillance;
- a description of categories of persons whose communications may be monitored;
- specifications of the maximum duration of surveillance;
- procedural details regarding analysis, use and storage of the acquired data;
- specifications of the precautions governing the disclosure of data to third parties;
- and details on when and how the collected data are deleted or notes should be destroyed.

In this case, the ECHR found that the Act in fact listed the specific criminal offences for whose prevention surveillance could be ordered for a maximum of 6 months. Accordingly, disclosure and use of personal data were permitted, since the provisions regarding the process, precautions regarding disclosure of the data and deletion of the data were specifically set down in the Act: the restrictions set down in the Act provided sufficient guarantees against arbitrary acts and the risk of abuses. Accordingly, the ECHR did not find a violation of Article 8.

In 2016, the provisions of the G-10 Act were tightened once more. Again, a complaint was lodged. At the time of writing, this complaint is still pending before the German Federal Constitutional Court.

## CASE EXAMPLE

# DISCLOSING DATA WHEN BUYING A SIM CARD

**Personal data must be provided by buyers of SIM cards if the telecommunications provider is obliged to collect this data.**

According to the German Telecommunications Act (TKG), every person wishing to purchase a prepaid SIM card is required to provide personal data, such as their name and address. Since 2004, telecommunications providers have been obliged to store this data and make it available to official authorities.

German politician Patrick Breyer lodged a complaint against this before the ECHR. He claimed

that the TKG breached the right to respect of privacy under Article 8, since it required proof of identity when purchasing a prepaid SIM card. This meant the buyer was not able to freely decide whether to provide their name, address and date of birth.

The ECHR dismissed the complaint. The court ruled that the provisions of the TKG did infringe on privacy as defined in Article 8 but were nonetheless justified in a democratic society: collecting personal data from a person purchasing a prepaid SIM card was a proportionate means for combatting crime and terrorism. A six-month period of data storage was also proportionate, the court said. The judgment was referred to the Grand Chamber and is pending before the chamber at the time of writing.



Surveillance measures must be foreseeable and therefore explicitly specified in the law. In individual cases, the persons concerned must have the possibility of having a surveillance report reviewed by a court.

# 'INSURANCE SPIES'

**The use of private detectives in the area of accident insurance must be based on explicit legal provisions.**

In Switzerland, Ms. Vukota-Bojić received benefit payments from the State accident insurance agency SUVA following an accident. After some time, the case of Ms. Vukota-Bojić was reassessed, and the insurer decided there was no further entitlement. Ms. Vukota-Bojić should therefore have her work incapacity reassessed, it said, which she refused to do. The insurer then had Ms. Vukota-Bojić surveilled by a private detective, which Ms. Vukota-Bojić objected to. The Swiss Federal Court concluded that the observation was justified. Ms. Vukota-Bojić took that judgment to the ECHR.

The ECHR determined firstly that the observation of a person by the State insurance provider was an infringement of her privacy under Article 8 of the European Convention on Human Rights. It further determined that such observation and the use of cameras would have had to be foreseeable for the person concerned; the law should have explicitly specified such measures.

Since the legislation specified neither a maximum duration of the surveillance nor the possibility of a review, the accident insurer had an excessive margin of discretion, it said. Accordingly the ECHR ruled that the surveillance violated Article 8.

Switzerland has subsequently further detailed the legal provisions in question, stating the specific measures involved.

# THE ECHR HAS FOUND IN MY FAVOUR – WHAT HAPPENS NOW?

The judgments of the ECHR have to be implemented by the national authorities. The decisions of the ECHR in Strasbourg are legally binding. However, all the ECHR can do is determine that there has been a violation of the Convention and award indemnification to the victim. It is not able to revoke any national laws that are contrary to human rights or to release individuals from prison. Implementation of its judgments is instead in the hands of the authorities of the member state in question.

# DOCUMENTATION

This brochure is part of our series on the ECHR's jurisprudence on different areas of life.

Previous brochures:

- The European Court of Human Rights and Freedom of Expression on the Internet (2020; English, German, French)
- The European Court of Human Rights and the Right to a Fair Trial (2018; German, French, Italian)
- The European Court of Human Rights - Protecting Businesses (2017; English, German, French, Italian)
- The European Court of Human Rights and Freedom of the Media in Switzerland (2016; German, French, Italian)

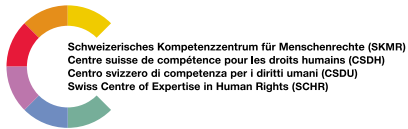
The brochures are available at

[www.csdh.ch](http://www.csdh.ch) > **publications**

Layout: **do2** Dominik Hunziker  
Cover photo: © ECHR-CEDH Council of Europe

 Entire brochure

 Contents



February 2021  
Swiss Centre of Expertise in Human Rights  
Schanzeneckstrasse 1, P.O. Box, 3001 Berne