July 2023
This factsheet does not bind the Court and is not exhaustive

Personal data protection

"The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of **Article 8** [**of the European Convention on Human Rights**, which guarantees the right to respect for private and family life, home and correspondence[1]] ... The subsequent use of the stored information has no bearing on that finding ... However, in determining whether the personal information retained by the authorities involves any ... private-life [aspect] ..., the [European] Court [of Human Rights] will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ..." (*S. and Marper v. the United Kingdom*, judgment (Grand Chamber) of 4 December 2008, § 67)

Collection of personal data

Data collected during door-to-door preaching

Jehovah's Witnesses v. Finland

9 May 2023[2]

This case concerned the obligation for individual Jehovah's Witnesses to obtain consent when collecting personal data during their door-to-door preaching. The applicant community complained, in particular, of the lack of an oral hearing in the domestic proceedings, and of the prohibition on note-taking without the consent of the interlocutor while evangelising.

The Court held that there had been **no violation of Article 9** (freedom of religion) of the Convention, finding that the domestic authorities had correctly balanced the interests of the applicant community with the rights of individuals as regards their personal information, holding that obtaining consent had been necessary. The Court noted, in particular, that the relevant law had applied to all religious communities, and that no fine had been imposed on the Jehovah's Witness community in this particular case. It considered that the requirement to obtain consent was necessary in order to prevent disclosure of personal and sensitive data, and that requirement had not hindered the Jehovah's Witnesses' freedom of religion. The Court also held that there had been **no violation of Article 6** (right to a fair trial) of the Convention, finding that, looked at holistically, the applicant community had had every opportunity to put forward evidence and make arguments over the seven years that the issue had been before the national authorities, and that the legal issues at stake had not required an oral hearing for their examination.

[1]. Article 8 of the European Convention on Human Rights provides that:
"1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[2]. This judgment will become final in the circumstances set out in Article 44 § 2 (final judgments) of the European Convention on Human Rights.

Data reflecting sexual orientation

Drelon v. France

8 September 2022

This case (two applications) concerned, first, the collection and retention, by the French blood donation service (EFS) of personal data reflecting the applicant's presumed sexual orientation – together with the rejection of his criminal complaint for discrimination – and, second, the refusal of his offers to donate blood, together with the dismissal by the *Conseil d'État* of his judicial review application challenging an order of 5 April 2016 which amended the selection criteria for blood donors.

The Court held that there had been a **violation of Article 8** of the Convention on account of the collection and retention of the personal data concerned. Addressing the first application, it considered that the collection and retention of sensitive personal data constituted an interference with the applicant's right to respect for his private life. That interference had a foreseeable legal basis as the authorities' discretionary power to set up a health database for such purpose was sufficiently regulated by the then applicable Law of 6 January 1978. Whilst the collection and retention of personal data concerning blood donor candidates contributed to guaranteeing blood safety, it was nevertheless particularly important for the sensitive data involved to be accurate, up-to-date, pertinent and non-excessive in relation to the goals pursued; and the data retention period had to be limited to what was necessary. The Court observed, first, that even though the applicant had refused to answer the questions about his sex life during the medical examination prior to the blood donation, the data included a contraindication to giving blood that was specific to men who had intercourse with other men. It concluded that the data in question was based on mere speculation without any proven factual basis. Secondly, after noting that the Government had not shown that the data retention period (until 2278 at the time) had been regulated in such a way that it could not exceed the period necessary for the aim pursued, the Court found that the excessive retention period had made it possible for the data to be used repeatedly against the applicant, thus entailing his automatic exclusion from being a blood donor. As to the second application, the Court **rejected** as out of time the complaints about the decisions excluding the applicant from blood donation on 16 November 2004 and 9 August 2006. As regards the decision of 26 May 2016 the Court found that the applicant could not invoke a violation of Articles 8 and 14 (prohibition of discrimination) of the Convention in respect of the order of 5 April 2016 as it was not yet in force on the date of the refusal in question.

DNA information and fingerprints

See below, under "Storage and use of personal data", "In the context of police and criminal justice".

GPS data

Uzun v. Germany

2 September 2010

The applicant, suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his right to respect for private life.

The Court held that there had been **no violation of Article 8** of the Convention. The GPS surveillance and the processing and use of the data thereby obtained had admittedly interfered with the applicant's right to respect for his private life. However, the Court noted, it had pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime. It had also been proportionate: GPS surveillance had been ordered only after less intrusive methods of

investigation had proved insufficient, had been carried out for a relatively short period (some three months), and had affected the applicant only when he was travelling in his accomplice's car. The applicant could not therefore be said to have been subjected to total and comprehensive surveillance. Given that the investigation had concerned very serious crimes, the applicant's surveillance by GPS had thus been necessary in a democratic society.

Ben Faiza v. France

8 February 2018

This case concerned surveillance measures taken against the applicant in a criminal investigation into his involvement in drug-trafficking offences. The applicant alleged that these measures (both the installation of a geolocation device on his vehicle and the court order issued to a mobile telephone operator to obtain records of his incoming and outgoing calls, together with the cell tower pings from his telephones, thus enabling the subsequent tracking of his movements) had constituted an interference with his right to respect for his private life.

The Court held that there had been a **violation of Article 8** of the Convention as regards the real-time geolocation of the applicant's vehicle by means of a GPS device on 3 June 2010, finding that, in the sphere of real-time geolocation measures, French law (neither statute law nor case-law) did not at the relevant time indicate with sufficient clarity to what extent and how the authorities were entitled to use their discretionary power. The applicant had therefore not enjoyed the minimum protection afforded by the rule of law in a democratic society. The Court noted, however, that subsequently France had adopted a legislative mechanism governing the use of geolocation and strengthening the right to respect for privacy (Law of 28 March 2014). The Court further held that there had been **no violation of Article 8** concerning the court order issued to a mobile telephone operator on 24 July 2009 to obtain the list of cell towers pinged by the applicant's phone for subsequent tracking of his movements. It noted in particular that the court order had constituted an interference with the applicant's private life but was in accordance with the law. Further, the order had been aimed at establishing the truth in the context of criminal proceedings for the importing of drugs in an organised gang, criminal conspiracy and money laundering, and had thus pursued the legitimate aims of preventing disorder or crime or protecting public health. The Court also considered that the measure had been necessary in a democratic society because it was aimed at breaking up a major drug-trafficking operation. Lastly, the information obtained had been used in an investigation and a criminal trial during which the applicant had been guaranteed an effective review consistent with the rule of law.

Florindo de Almeida Vasconcelos Gramaxo v. Portugal

13 December 2022

This case concerned the applicant's dismissal on the basis of data obtained from a geolocation system fitted in the car which his employer had made available to him for the purposes of his work as a medical representative. The applicant submitted that the processing of geolocation data obtained from the GPS system installed in his company vehicle, and the use of that data as the basis for his dismissal, had infringed his right to respect for his private life. He also complained that the proceedings before the domestic courts had been unfair, as the courts' decisions had been based almost exclusively on unlawful evidence obtained by means of the GPS system installed in his company vehicle.

The Court held that there had been **no violation of Article 8** of the Convention, finding that the national authorities had not failed to comply with their positive obligation to protect the applicant's right to respect for his private life. It observed at the outset that the applicant had been aware that the company had installed a GPS system in his vehicle with the aim of monitoring the distances travelled in the course of his professional activity and, as applicable, on private journeys. It also noted that, by taking into account only the geolocation data relating to the distances travelled, the Court of Appeal had reduced the extent of the intrusion into the applicant's private life to what was strictly

necessary to achieve the legitimate aim pursued, namely to monitor the company's expenditure. In the applicant's case, the Court considered that the Court of Appeal had carried out a detailed balancing exercise between the applicant's right to respect for his private life and his employer's right to ensure the smooth running of the company, taking into account the legitimate aim pursued by the company, namely the right to monitor its expenditure. Hence, the State had not overstepped its margin of appreciation in the present case. The Court also held that there had been **no violation of Article 6 § 1** (right to a fair trial) of the Convention, finding that the use in evidence of the geolocation data relating to the distances driven by the applicant in his company vehicle had not undermined the fairness of the proceedings in the present case.

Health data

L.H. v. Latvia (no. 52019/07)

29 April 2014

The applicant alleged in particular that the collection of her personal medical data by a State agency – in this case, the Inspectorate of Quality Control for Medical Care and Fitness for Work ("MADEKKI") – without her consent had violated her right to respect for her private life.

In this judgment the Court recalled the importance of the protection of medical data to a person's enjoyment of the right to respect for private life. It held that there had been a **violation of Article 8** of the Convention in the applicant's case, finding that the applicable law had failed to indicate with sufficient clarity the scope of discretion conferred on competent authorities and the manner of its exercise. The Court noted in particular that Latvian law in no way limited the scope of private data that could be collected by MADEKKI, which resulted in it collecting medical data on the applicant relating to a seven-year period indiscriminately and without any prior assessment of whether such data could be potentially decisive, relevant or of importance for achieving whatever aim might have been pursued by the inquiry at issue.

Y.G. v. Russia (no. 8647/12)[3]

30 August 2022

See below, under "Disclosure of personal data".

Interception of communications, phone tapping and secret surveillance

Klass and Others v. Germany

6 September 1978

In this case the applicants, five German lawyers, complained in particular about legislation in Germany empowering the authorities to monitor their correspondence and telephone communications without obliging the authorities to inform them subsequently of the measures taken against them.

The Court held that there had been **no violation of Article 8** of the Convention, finding that the German legislature was justified to consider the interference resulting from the contested legislation with the exercise of the right guaranteed by Article 8 § 1 as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime (Article 8 § 2). The Court observed in particular that powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions. Noting, however, that democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to

[3]. On 16 September 2022 the Russian Federation ceased to be a Party to the European Convention on Human Rights ("the Convention").

undertake the secret surveillance of subversive elements operating within its jurisdiction, the Court considered that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

Malone v. the United Kingdom

2 August 1984

Charged with a number of offences relating to dishonest handling of stolen goods, the applicant complained in particular of the interception of his postal and telephone communications by or on behalf of the police, and of the "metering" of his telephone (a process involving the use of a device which registers the numbers dialled on a particular telephone and the time and duration of each call).

The Court held that there had been a **violation of Article 8** of the Convention, as regards both interception of communications and release of records of metering to the police, because they had not been in accordance with the law.

Kruslin v. France

24 April 1990

This case concerned a telephone tapping ordered by an investigating judge in a murder case.

The Court held that there had been a **violation of Article 8** of the Convention, finding that French law did not indicate with reasonable clarity the scope and manner of exercise of the authorities' discretion in this area. This was truer still at the material time, so that the Court considered that the applicant had not enjoyed the minimum degree of protection to which citizens are entitled under the rule of law in a democratic society.

See also, among others: **Huvig v. France**, judgment of 24 April 1990; **Halford v. the United Kingdom**, judgment of 25 June 1997.

Kopp v. Switzerland

25 March 1998

This case concerned the monitoring of the applicant's law firm's telephone lines on orders of the Federal Public Prosecutor.

The Court held that there had been a **violation of Article 8** of the Convention, finding that Swiss law did not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. The Court consequently considered that the applicant, as a lawyer, had not enjoyed the minimum degree of protection required by the rule of law in a democratic society.

Amann v. Switzerland

16 February 2000 (Grand Chamber)

This case concerned a telephone call to the applicant from the former Soviet embassy – to order a depilatory appliance advertised by him – intercepted by the public prosecutor's office, which requested the intelligence service to draw up a file on the applicant.

The Court held that there had been a **violation of Article 8** of the Convention on account of the recording of the telephone call and a **violation of the same provision** on account of the creation and storage of the file, finding that these interferences with the applicant's right to respect for his private life were not in accordance with the law, since Swiss law was unclear as to the authorities' discretionary power in this area.

Taylor-Sabori v. the United Kingdom

22 October 2002

This case concerned in particular the interception by the police, as part of a covert surveillance operation, of messages sent to the applicant's pager.

The Court held there had been a **violation of Article 8** of the Convention. Noting in particular that, at the time of the events in question, there was no statutory

system to regulate the interception of pager messages transmitted via a private telecommunication system, it found, as the UK Government had accepted, that the interference was not in accordance with the law.

Wisse v. France

22 December 2005

The two applicants were arrested on suspicion of committing armed robberies and placed in pre-trial detention. Under a warrant issued by the investigating judge, the telephone conversations between them and their relatives in the prison visiting rooms were recorded. The applicants made an unsuccessful application to have the steps in the proceedings relating to the recording of their conversations declared invalid. They argued that the recording of their conversations in the prison visiting rooms had constituted interference with their right to respect for their private and family life.

The Court held that there had been a **violation of Article 8** of the Convention, finding that French law did not indicate with sufficient clarity how and to what extent the authorities could interfere with detainees' private lives, or the scope and manner of exercise of their powers of discretion in that sphere. Consequently, the applicants had not enjoyed the minimum degree of protection required by the rule of law in a democratic society. The Court noted in particular that, the systematic recording of conversations in a visiting room for purposes other than prison security deprived visiting rooms of their sole *raison d'être*, namely to allow detainees to maintain some degree of private life, including the privacy of conversations with their families.

Kennedy v. the United Kingdom

18 May 2010

Convicted of manslaughter – in a case which was controversial on account of missing and conflicting evidence – and released from prison in 1996, the applicant subsequently became active in campaigning against miscarriages of justice. Suspecting police interception of his communications after he had started a small business, he complained to the Investigatory Powers Tribunal (IPT). He was eventually informed in 2005 that no determination had been made in his favour in respect of his complaints. This meant either that his communications had not been intercepted or that the IPT considered any interception to be lawful. No further information was provided by the IPT. The applicant complained about the alleged interception of his communications.

The Court held that there had been **no violation of Article 8** of the Convention, finding that UK law on interception of internal communications together with the clarifications brought by the publication of a Code of Practice indicated with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of data collected. Moreover, there was no evidence of any significant shortcomings in the application and operation of the surveillance regime. Therefore, and having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, in so far as they might have been applied to the applicant, had been justified under Article 8 § 2 of the Convention.

Dragojević v. Croatia

15 January 2015

This case principally concerned the secret surveillance of telephone conversations of a drug-trafficking suspect. The applicant alleged in particular that the investigating judge had failed to comply with the procedure required by Croatian law to effectively assess whether the use of secret surveillance was necessary and justified in his particular case.

The Court held that there had been a **violation of Article 8** of the Convention. It found in particular that Croatian law, as interpreted by the national courts, did not provide reasonable clarity as to the authorities' discretion in ordering surveillance measures and it did not in practice – as applied in the applicant's case – provide sufficient safeguards against possible abuse.

See also: **Bašić v. Croatia**, judgment of 25 October 2016; **Matanović v. Croatia**, judgment of 4 April 2017.

R.E. v. the United Kingdom (no. 62498/11)

27 October 2015

The applicant, who was arrested and detained in Northern Ireland on three occasions in connection with the murder of a police officer, complained in particular about the regime for covert surveillance of consultations between detainees and their lawyers and between vulnerable detainees[4] and "appropriate adults"[5].

This case was considered from the standpoint of the principles developed by the Court in the area of interception of lawyer-client telephone calls, which call for stringent safeguards. The Court found that those principles should be applied to the covert surveillance of lawyer-client consultations in a police station. In the present case, the Court held that there had been a **violation of Article 8** of the Convention as concerned the covert surveillance of legal consultations. It noted in particular that guidelines arranging for the secure handling, storage and destruction of material obtained through such covert surveillance had been implemented since 22 June 2010. However, at the time of the applicant's detention in May 2010, those guidelines had not yet been in force. The Court was not therefore satisfied that the relevant domestic law provisions in place at the time had provided sufficient safeguards for the protection of the applicant's consultations with his lawyer obtained by covert surveillance. The Court further held that there had been **no violation of Article 8** as concerned the covert surveillance of consultations between detainees and their "appropriate adults", finding in particular that they were not subject to legal privilege and therefore a detainee would not have the same expectation of privacy as for a legal consultation. Furthermore, the Court was satisfied that the relevant domestic provisions, insofar as they related to the possible surveillance of consultations between detainees and "appropriate adults", were accompanied by adequate safeguards against abuse.

Roman Zakharov v. Russia[6]

4 December 2015 (Grand Chamber)

This case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as well as for storing and destroying the intercepted data; the supervision of the interception. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception and that obtaining such proof was impossible in the absence of any notification system or possibility of access to information about interception.

---

4. A juvenile or person who is mentally disordered or otherwise mentally vulnerable
5. An "appropriate adult" could be a relative or guardian, or a person experienced in dealing with mentally disordered or mentally vulnerable people.
6. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

See also, concerning secret surveillance measures in the context of criminal proceedings: **Akhlyustin v. Russia**, **Zubkov and Others v. Russia**, **Moskalev v. Russia** and **Konstantin Moskalev v. Russia**, judgments of 7 November 2017[7].

Szabó and Vissy v. Hungary

12 January 2016

This case concerned Hungarian legislation on secret anti-terrorist surveillance introduced in 2011. The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes (namely, "section 7/E (3) surveillance"). They notably alleged that this legal framework was prone to abuse, notably for want of judicial control.

In this case the Court held that there had been a **violation of Article 8** of the Convention. It accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the measures could include virtually anyone in Hungary, with new technologies enabling the Government to intercept masses of data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place. The Court further held that there had been **no violation of Article 13** (right to an effective remedy) of the Convention **taken together with Article 8**, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.

Mustafa Sezgin Tanrıkulu v. Turkey

18 July 2017

The applicant complained about a domestic court decision of 2005 allowing the interception of communications of anyone in Turkey, including himself, for about a month and a half. He alleged in particular that the interception measures amounted to abuse of the national legislation in force at the time. He also claimed that he had been denied an effective judicial remedy because the national authorities had refused to carry out an investigation into his complaints about the interception of his communications.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the interception order in the present case was not in accordance with the law. The Court also held that there had been a **violation of Article 13** (right to an effective remedy) of the Convention**.**

Ben Faiza v. France

8 February 2018

See above, under "GPS data".

Benedik v. Slovenia

24 April 2018

This case concerned the Slovenian police's failure to obtain a court order to access subscriber information associated with a dynamic IP address recorded by the Swiss law-enforcement authorities during their monitoring of users of a certain file-sharing network. This led to the applicant being identified after he had shared files over the network, including child pornography.

The Court held that there had been a **violation of Article 8** of the Convention. It found in particular that the legal provision used by the police to obtain the subscriber information associated with the dynamic IP address had not met the Convention

[7]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

standard of being "in accordance with the law". The provision had lacked clarity, offered virtually no protection from arbitrary interference, had no safeguards against abuse and no independent supervision of the police powers involved.

Hambardzumyan v. Armenia

5 December 2019

The applicant alleged that the police had not had a valid court warrant to place her under secret surveillance during a criminal investigation. She complained in particular about the covert surveillance and its subsequent use in the criminal proceedings against her.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the surveillance measure used against the applicant had not had proper judicial supervision and had not been "in accordance with the law" within the meaning of the Convention. It noted in particular that the warrant had not been specific enough about the person who was the object of the surveillance measure, vagueness which was unacceptable when it came to such a serious interference with the right to respect for private and family life as secret surveillance. Furthermore, the warrant had not listed the specific measures that were to be carried out against the applicant. The Court held, however, that there had been **no violation of Article 6** (right to a fair trial) of the Convention in the applicant's case, finding that the use of the secretly taped material had not conflicted with the requirements of fairness guaranteed by Article 6 § 1.

Privacy International and Others v. the United Kingdom

7 July 2020 (decision on the admissibility)

The applicants – an NGO registered in London, an Internet service provider registered in London, an association of "hacktivists" registered in Germany, two companies registered in the United States providing Internet services and communications services respectively, and an Internet service provider registered in South Korea – believed that their equipment had been subject to interference, colloquially known as "hacking", over an undefined period by the United Kingdom Government Communications Headquarters and/or the Secret Intelligence Service. They complained in particular that the power under Section 7 of the Intelligence Services Act[8] was not in accordance with the law, that it contained no requirement for judicial authorisation, that there was no information in the public domain about how it might be used to authorise Equipment Interference, and that there was no requirement for filtering to exclude irrelevant material. They added that the Investigatory Powers Tribunal did not provide an effective remedy as it did not rule on the Section 7 regime in the domestic litigation.

The Court declared the applicants' complaints under Article 8, Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention **inadmissible**, finding that, in the circumstances of the case, the applicants had not provided the domestic courts, notably the Investigatory Powers Tribunal, with the opportunity which is in principle intended by Article 35 (admissibility criteria) of the Convention to be afforded to a Contracting State, namely the opportunity of addressing, and thereby preventing or putting right, the particular Convention violation alleged against it. The Court noted in particular the general arguments advanced by the applicants and also underlined in the interventions of the third parties that the surveillance complained of was particularly intrusive and that there was a need for safeguards in this domain. In that respect, it recalled the importance of examining compliance with the principles of Article 8 of the Convention where the powers vested in the State are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated. However, that importance reinforced in the context of exhaustion of domestic remedies the need to provide the domestic courts with the possibility to rule on such matters where they have the potential to do so.

[8]. Section 7 of the Intelligence Services Act 1994 ("the ISA") allows the Secretary of State to authorise a person to undertake (and to exempt them from liability for) an act outside the British Islands in relation to which they would be liable if it were done in the United Kingdom.

Big Brother Watch and Others v. the United Kingdom

25 May 2021 (Grand Chamber)

These applications were lodged after revelations by Edward Snowden (former contractor with the US National Security Agency) about programmes of surveillance and intelligence sharing between the USA and the United Kingdom. The case concerned complaints by journalists and human-rights organisations in regard to three different surveillance regimes: (1) the bulk interception of communications; (2) the receipt of intercept material from foreign governments and intelligence agencies; (3) the obtaining of communications data from communication service providers[9].

The Grand Chamber held: unanimously, that there had been a **violation of Article 8** of the Convention in respect of the bulk intercept regime; unanimously, that there had been a **violation of Article 8** in respect of the regime for obtaining communications data from communication service providers; by twelve votes to five, that there had been **no violation of Article 8** in respect of the United Kingdom's regime for requesting intercepted material from foreign Governments and intelligence agencies; unanimously, that there had been a **violation of Article 10** (freedom of expression) of the Convention, concerning both the bulk interception regime and the regime for obtaining communications data from communication service providers; and, by twelve votes to fives, that there had been **no violation of Article 10** in respect of the regime for requesting intercepted material from foreign Governments and intelligence agencies. The Court considered in particular that, owing to the multitude of threats States face in modern society, operating a bulk interception regime did not in and of itself violate the Convention. However, such a regime had to be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation were being defined; and that the operation should be subject to supervision and independent ex post facto review. Having regard to the bulk interception regime operated in the UK, the Court identified the following deficiencies: bulk interception had been authorised by the Secretary of State, and not by a body independent of the executive; categories of search terms defining the kinds of communications that would become liable for examination had not been included in the application for a warrant; and search terms linked to an individual (that is to say specific identifiers such as an email address) had not been subject to prior internal authorisation. The Court also found that the bulk interception regime had not contained sufficient protections for confidential journalistic material. The regime for obtaining communications data from communication service providers was also found to have not been in accordance with the law. However, the Court held that the regime by which the UK could request intelligence from foreign governments and/or intelligence agencies had had sufficient safeguards in place to protect against abuse and to ensure that UK authorities had not used such requests as a means of circumventing their duties under domestic law and the Convention.

Centrum För Rättvisa v. Sweden

25 May 2021 (Grand Chamber)

This case concerned the alleged risk that the applicant foundation's communications had been or would be intercepted and examined by way of signals intelligence, as it communicated on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax, often on sensitive matters.

The Grand Chamber held, by fifteen votes to two, that there had been a **violation of Article 8** of the Convention. It found, in particular, that although the main features of

[9]. At the relevant time, the regime for bulk interception and obtaining communications data from communication service providers had a statutory basis in the Regulation of Investigatory Powers Act 2000. This had since been replaced by the Investigatory Powers Act 2016. The findings of the Grand Chamber relate solely to the provisions of the 2000 Act, which had been the legal framework in force at the time the events complained of had taken place.

the Swedish bulk interception regime met the Convention requirements on quality of the law, the regime nevertheless suffered from three defects: the absence of a clear rule on destroying intercepted material which did not contain personal data; the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration was given to the privacy interests of individuals; and the absence of an effective ex post facto review. As a result of these deficiencies, the system did not meet the requirement of "end-to-end" safeguards, it overstepped the margin of appreciation left to the respondent State in that regard, and overall did not guard against the risk of arbitrariness and abuse.

See also, recently:

Ringler v. Austria

12 May 2020 (Committee – decision on the admissibility)

Tretter and Others v. Austria

29 September 2020 (Committee – decision on the admissibility)

Adomaitis v. Lithuania

18 January 2022

Pending applications

Association confraternelle de la presse judiciaire v. France and 11 other applications (nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15)

Applications communicated to the French Government on 26 April 2017

These applications, which were lodged by lawyers and journalists, as well as legal persons connected with these professions, concern the French Intelligence Act of 24 July 2015.

The Court gave notice of the applications to the French Government and put questions to the parties under Articles 8, 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.

Similar applications pending: **Follorou v. France (no. 30635/17) and Johannes v. France (no. 30636/17)**, communicated to the French Government on 4 July 2017.

Pietrzak v. Poland (no. 72038/17) and Bychawska-Siniarska and Others v. Poland (no. 25237/18)

Applications communicated to the Polish Government on 27 November 2019

These applications concern the Polish legislation authorising a system of secret surveillance of telephone, postal and electronic communications and the collection of data relating to these communications ('metadata').

In November 2019 the Court gave notice of the applications to the Polish Government and put questions to the parties under Articles 8 (right to respect for private life and correspondence) and 13 (right to an effective remedy) of the Convention.

Eleven third-party interveners have been given leave to take part in the written procedure; of these, four have been invited to take part in the Chamber hearing which took place in the Human Rights Building on 27 September 2022.

A.L. v. France (no. 44715/20) and E.J. v. France (no. 47930/21)

Applications communicated to the French Government on 8 December 2021

These applications concern in particular the infiltration by the French authorities of the encrypted communication network "EncroChat" and the capture, copying and analysis of data stored and exchanged with the devices connected to this network.

The Court gave notice of the applications to the French Government and put questions to the parties under Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life

and correspondence), 13 (right to an effective remedy), 34 (right of individual application) and 35 (admissibility criteria) of the Convention.

Monitoring of employees' computer use

Bărbulescu v. Romania

5 September 2017 (Grand Chamber)

This case concerned the decision of a private company to dismiss an employee – the applicant – after monitoring his electronic communications and accessing their contents. The applicant complained that his employer's decision was based on a breach of his privacy and that the domestic courts had failed to protect his right to respect for his private life and correspondence.

The Grand Chamber held, by eleven votes to six, that there had been a **violation of Article 8** of the Convention, finding that the Romanian authorities had not adequately protected the applicant's right to respect for his private life and correspondence. They had consequently failed to strike a fair balance between the interests at stake. In particular, the national courts had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; nor had they had regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or the degree of intrusion into his private life and correspondence. In addition, the national courts had failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge.

Libert v. France

22 February 2018

This case concerned the dismissal of an SNCF (French national railway company) employee after the seizure of his work computer had revealed the storage of pornographic files and forged certificates drawn up for third persons. The applicant complained in particular that his employer had opened, in his absence, personal files stored on the hard drive of his work computer.

The Court held that there had been **no violation of Article 8** of the Convention, finding that in the present case the French authorities had not overstepped the margin of appreciation available to them. The Court noted in particular that the consultation of the files by the applicant's employer had pursed a legitimate aim of protecting the rights of employers, who might legitimately wish to ensure that their employees were using the computer facilities which they had placed at their disposal in line with their contractual obligations and the applicable regulations. The Court also observed that French law comprised a privacy protection mechanism allowing employers to open professional files, although they could not surreptitiously open files identified as being personal. They could only open the latter type of files in the employee's presence. The domestic courts had ruled that the said mechanism would not have prevented the employer from opening the files at issue since they had not been duly identified as being private. Lastly, the Court considered that the domestic courts had properly assessed the applicant's allegation of a violation of his right to respect for his private life, and that those courts' decisions had been based on relevant and sufficient grounds.

Saliva samples

Dragan Petrović v. Serbia

14 April 2020

This case concerned a police search of the applicant's flat and the taking of a saliva sample from him for a DNA analysis during a murder investigation. The applicant

complained that the search and taking of the DNA sample had violated his rights protected by the Convention.
The Court held that there had been **no violation of Article 8** of the Convention as regards the police search of the applicant's apartment, finding that the search warrant had been specific enough and had been attended by adequate and effective safeguards against abuse during the search itself. It held, however, that there had been a **violation of Article 8** owing to the taking of a DNA saliva sample from the applicant, finding that the taking of the DNA saliva sample had not been "in accordance with the law" within the meaning of Article 8. The measure had been carried out under a previous Code of Criminal Procedure, which had only authorised that blood samples could be taken, or "other medical procedures" carried out. Furthermore, the Court noted that the Code had been updated in 2011 with new safeguards related to DNA mouth swabs, an implicit acknowledgement that they had been lacking previously.

Voice samples

P.G. and J.H. v. the United Kingdom (no. 44787/98)

25 September 2001
This case concerned in particular the recording of the applicants' voices at a police station, following their arrest on suspicion of being about to commit a robbery.
The Court held that there had been a **violation of Article 8** of the Convention concerning the use of covert listening devices at the police station. Noting in particular that, at the relevant time, there existed no statutory system to regulate the use of covert listening devices by the police on their own premises, the Court found the interference with the applicants' right to a private life was not in accordance with the law. In this case the Court also found a **violation of Article 8** on account of the use of a covert listening device at a flat and **no violation of Article 8** as regards obtaining of information about the use of a telephone.

Vetter v. France

31 May 2005
Following the discovery of a body with gunshot wounds, the police, suspecting that the applicant had carried out the murder, installed listening devices in a flat to which he was a regular visitor.
The Court held that there had been a **violation of Article 8** of the Convention, finding that French law did not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in relation to listening devices.

Video surveillance

Peck v. the United Kingdom

28 January 2003
See below, under "Disclosure of personal data".

Köpke v. Germany

5 October 2010 (decision on the admissibility)
The applicant, a supermarket cashier, was dismissed without notice for theft, following a covert video surveillance operation carried out by her employer with the help of a private detective agency. She unsuccessfully challenged her dismissal before the labour courts. Her constitutional complaint was likewise dismissed.
The Court rejected the applicant's complaint under Article 8 of the Convention as **inadmissible** (manifestly ill-founded). It concluded that the domestic authorities had struck a fair balance between the employee's right to respect for her private life and her employer's interest in the protection of its property rights and the public interest in the proper administration of justice. The Court observed, however, that the competing interests concerned might well be given a different weight in the future, having regard to

the extent to which intrusions into private life were made possible by new, more and more sophisticated technologies.

Antović and Mirković v. Montenegro

28 November 2017

This case concerned an invasion of privacy complaint by two professors at the University of Montenegro's School of Mathematics after video surveillance had been installed in areas where they taught. They stated that they had had no effective control over the information collected and that the surveillance had been unlawful. The domestic courts rejected a compensation claim however, finding that the question of private life had not been at issue as the auditoriums where the applicants taught were public areas.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the camera surveillance had not been in accordance with the law. It first rejected the Government's argument that the case was inadmissible because no privacy issue had been at stake as the area under surveillance had been a public, working area. In this regard the Court noted in particular that it had previously found that private life might include professional activities and considered that was also the case with the applicants. Article 8 was therefore applicable. On the merits of the case, the Court then found that the camera surveillance had amounted to an interference with the applicants' right to privacy and that the evidence showed that that surveillance had violated the provisions of domestic law. Indeed, the domestic courts had never even considered any legal justification for the surveillance because they had decided from the outset that there had been no invasion of privacy.

López Ribalda and Others v. Spain

17 October 2019 (Grand Chamber)

This case concerned the covert video-surveillance of employees which led to their dismissal. The applicants complained about the covert video-surveillance and the Spanish courts' use of the data obtained to find that their dismissals had been fair. The applicants who signed settlement agreements also complained that the agreements had been made under duress owing to the video material and should not have been accepted as evidence that their dismissals had been fair.

The Grand Chamber held that there had been **no violation of Article 8** of the Convention in respect of the five applicants. It found in particular that the Spanish courts had carefully balanced the rights of the applicants – supermarket employees suspected of theft – and those of the employer, and had carried out a thorough examination of the justification for the video-surveillance. A key argument made by the applicants was that they had not been given prior notification of the surveillance, despite such a legal requirement, but the Court found that there had been a clear justification for such a measure owing to a reasonable suspicion of serious misconduct and to the losses involved, taking account of the extent and the consequences of the measure. In the present case the domestic courts had thus not exceeded their power of discretion ("margin of appreciation") in finding the monitoring proportionate and legitimate. The Court also held that there had been **no violation of Article 6 § 1** (right to a fair trial) of the Convention, finding in particular that the use of the video material as evidence had not undermined the fairness of the trial.

Storage and use of personal data

"The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and

not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... [It] must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse ..." (*S. and Marper v. the United Kingdom*, judgment (Grand Chamber) of 4 December 2008, § 103)

Biometric data

Glukhin v. Russia[10]

4 July 2023[11]

This case concerned the authorities' use of facial-recognition technology against the applicant following his holding a solo demonstration in the Moscow underground. He had been identified and later located by facial-recognition technology after travelling with a life-size cardboard figure of a protestor whose case had attracted widespread attention in the media, holding a banner that said, "I'm facing up to five years … for peaceful protests". The applicant submitted in particular that his administrative conviction and the use of facial-recognition technology in the processing of his personal data had breached his right to respect for private life and his freedom of expression.

The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention in respect of the applicant, finding that the processing of his biometric personal data using facial-recognition technology in the framework of administrative-offence proceedings – firstly, to identify him from the photographs and the video published on the Internet and, secondly, to locate and arrest him while he was travelling on the Moscow underground – had not corresponded to "a pressing social need" and could not be regarded as "necessary in a democratic society". The Court noted in particular that the measures taken against the applicant had been particularly intrusive in the face of what had been a peaceful protest, which had not presented any danger to the public or transport safety. It had in fact only led to his prosecution for a minor offence. The Court also held that there had been a **violation of Article 10** (freedom of expression) of the Convention in the present case, finding that the domestic courts had failed to provide "relevant or sufficient reasons" to justify escorting the applicant to the police station, arresting and convicting him.

In the context of criminal justice

Perry v. the United Kingdom

17 July 2003

The applicant was arrested in connection with a series of armed robberies of mini-cab drivers and released pending an identification parade. When he failed to attend that and several further identification parades, the police requested permission to video him covertly. The applicant complained that the police had covertly videotaped him for identification purposes and used the videotape in the prosecution against him.

The Court held that there had been a **violation** of Article 8 of the Convention. It noted that there had been no indication that the applicant had had any expectation that footage would be taken of him in the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. That ploy adopted by the police had gone beyond the normal use of this type of camera and amounted to an interference with the applicant's right to respect for his private life. The interference in question had further not been in accordance with the law because the police had failed to comply with the procedures set out in the applicable code: they had not obtained the applicant's consent or informed him that the tape was being made; neither had they informed him of his rights in that respect.

[10]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.
[11]. This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention.

S. and Marper v. the United Kingdom

4 December 2008 (Grand Chamber)

This case concerned the indefinite retention in a database of the applicants' fingerprints, cell samples and DNA profiles[12] after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the retention at issue had constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society. The Court considered in particular that the use of modern scientific techniques in the criminal-justice system could not be allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. Any State claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance". The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests.

B.B. v. France (no. 5335/06), Gardel v. France and M.B. v. France (no. 22115/06)

17 December 2009

The applicants in these cases, who had been sentenced to terms of imprisonment for rape of 15 year old minors by a person in a position of authority, complained in particular about their inclusion in the automated national judicial database of sex offenders (*Fichier judiciaire national automatisé des auteurs d'infractions sexuelles*).

In the three cases the Court held that there had been **no violation of Article 8** of the Convention, finding that the system of inclusion in the national judicial database of sex offenders, as applied to the applicants, had struck a fair balance between the competing private and public interests at stake. The Court reaffirmed in particular that the protection of personal data was of fundamental importance to a person's enjoyment of respect for his or her private and family life, all the more so where such data underwent automatic processing, not least when such data were used for police purposes. However, the Court could not call into question the prevention-related objectives of the database. Moreover, as the applicants had an effective possibility of submitting a request for the deletion of the data, the Court took the view that the length of the data conservation – 30 years maximum – was not disproportionate in relation to the aim pursued by the retention of the information. Lastly, the consultation of such data by the court, police and administrative authorities, was subject to a duty of confidentiality and was restricted to precisely determined circumstances.

See also: **J.P.D. v. France (no. 55432/10)**, decision (inadmissible) of 16 September 2014.

Uzun v. Germany

2 September 2010

See above, under "Collection of personal data", "GPS data".

Dimitrov-Kazakov v. Bulgaria

10 February 2011

The applicant's name was entered in the police registers, with reference to a rape, as an "offender", after being questioned about a rape, even though he had never been indicted for the offence. He was later subjected by the police to a number of checks related to rape complaints or disappearances of young girls. He complained about his inclusion in the police file and about the lack of a remedy by which to have that complaint examined.

[12]. DNA profiles are digitised information which is stored electronically on the National DNA Database together with details of the person to whom it relates.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the inclusion in the police file was not "in accordance with the law" within the meaning of that Article. It also held that there had been a **violation of Article 13** (right to an effective remedy) of the Convention **read in conjunction with Article 8**, on account of the lack of an effective remedy in that respect.

Shimovolos v. Russia[13]

21 June 2011

This case concerned the registration of a human rights activist in the so-called "surveillance database", which collected information about his movements, by train or air, within Russia, and his arrest.

The Court held that there had been a **violation of Article 8** of the Convention. It noted in particular that the creation and maintenance of the database and the procedure for its operation were governed by a ministerial order which had never been published or otherwise made accessible to the public. Consequently, the Court found that the domestic law did not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store information on individuals' private lives in the database. In particular, it did not set out in a form accessible to the public any indication of the minimum safeguards against abuse.

Khelili v. Switzerland

18 October 2011

The applicant in this case complained that since the discovery of her calling cards by the During a police check in 1993 the Geneva police found the applicant to be carrying calling cards which read: "Nice, pretty woman, late thirties, would like to meet a man to have a drink together or go out from time to time. Tel. no. …". The applicant alleged that, following this discovery, the police entered her name in their records as a prostitute, an occupation she consistently denied engaging in. She submitted that the storage of allegedly false data concerning her private life had breached her right to respect for her private life.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the storage in the police records of allegedly false data concerning her private life had breached the applicant's right to respect for her private life and that the retention of the word "prostitute" for years had neither been justified nor necessary in a democratic society. The Court observed in particular that the word at issue could damage the applicant's reputation and make her day-to-day life more problematic, given that the data contained in the police records might be transferred to the authorities. That was all the more significant because personal data was currently subject to automatic processing, thus considerably facilitating access to and the distribution of such data. The applicant therefore had a considerable interest in having the word "prostitute" removed from the police records.

M.M. v. the United Kingdom (no. 24029/07)

13 November 2012

In 2000 the applicant was arrested by the police after disappearing with her baby grandson for a day in an attempt to prevent his departure to Australia following the breakup of her son's marriage. The authorities decided not to prosecute and she was instead cautioned for child abduction. The caution was initially intended to remain on her record for five years, but owing to a change of policy in cases where the injured party was a child, that period was later extended to life. The applicant complained about the indefinite retention and disclosure of her caution data and the impact of this on her employment prospects.

The Court held that there had been a **violation of Article 8** of the Convention. Indeed, as a result of the cumulative effect of the shortcomings identified, it was not satisfied that there were sufficient safeguards in the system for retention and disclosure of

[13]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

criminal record data to ensure that data relating to the applicant's private life would not be disclosed in violation of her right to respect for her private life. The retention and disclosure of the applicant's caution data accordingly could not be regarded as having been in accordance with the law within the meaning of Article 8. The Court noted in particular that, although data contained in the criminal record were, in one sense, public information, their systematic storing in central records meant that they were available for disclosure long after the event when everyone other than the person concerned was likely to have forgotten about it, especially where, as in the applicant's case, the caution had occurred in private. Thus, as the conviction or caution itself receded into the past, it became a part of the person's private life which had to be respected.

M.K. v. France (no. 19522/09)

18 April 2013

In 2004 and 2005 the applicant was the subject of two investigations into the theft of some books. He was acquitted following the first set of proceedings and the second set of proceedings was discontinued. On both occasions his fingerprints were taken and recorded in the fingerprints database. In 2006 the applicant requested that his prints be deleted from the database. His request was granted only in relation to the prints taken during the first set of proceedings. The appeals lodged by the applicant were dismissed. The applicant complained that the retention of data concerning him in the computerised database of fingerprints had infringed his right to respect for his private life.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the retention of the data amounted to disproportionate interference with the applicant's right to respect for his private life and could not be said to be necessary in a democratic society. The Court noted in particular that the French State had overstepped its margin of appreciation in the matter as the system for retaining the fingerprints of persons suspected of an offence but not convicted, as applied to the applicant in the present case, did not strike a fair balance between the competing public and private interests at stake.

Peruzzo and Martens v. Germany

4 June 2013 (decision on the admissibility)

The applicants, who had been convicted of serious criminal offences, complained about the domestic courts' orders to collect cellular material from them and to store it in a database in the form of DNA profiles for the purpose of facilitating the investigation of possible future crimes.

The Court declared the application **inadmissible** as manifestly ill-founded. It found that the domestic rules on the taking and retention of DNA material from persons convicted of offences reaching a certain level of gravity as applied in the case of the applicants had struck a fair balance between the competing public and private interests and fell within the respondent State's acceptable margin of appreciation.

See also: **W. v. the Netherlands (no. 20689/08)**, decision (inadmissible) of 20 January 2009.

Brunet v. France

18 September 2014

The applicant complained in particular of an interference with his private life as a result of being added to the police database STIC (system for processing recorded offences) – containing information from investigation reports, listing the individuals implicated and the victims – after the discontinuance of criminal proceedings against him.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the French State had overstepped its discretion to decide ("margin of appreciation") on such matters: the retention could be regarded as a disproportionate breach of the applicant's right to respect for his private life and was not necessary in a democratic society. The Court considered in particular that the applicant had not had a real possibility of seeking the deletion from the database of the information concerning him

and that the length of retention of that data, 20 years, could be assimilated, if not to indefinite retention, at least to a norm rather than to a maximum limit.

Karabeyoğlu v. Turkey

7 June 2016

This case concerned a telephone surveillance operation in respect of the applicant, a public prosecutor, during a criminal investigation into an illegal organisation known as *Ergenekon*, and the use of the information thus obtained in the context of a separate disciplinary investigation.

The Court held that there had been **no violation of Article 8** of the Convention as regards the telephone tapping in connection with the criminal investigation and a **violation of Article 8** as regards the use in disciplinary proceedings of the information obtained by means of telephone tapping. The Court found in particular that during the criminal investigation the applicant had enjoyed the minimum degree of protection required by the rule of law in a democratic society, since the telephone tapping had been ordered on the basis of an objectively reasonable suspicion and had been carried out in compliance with the relevant legislation. In the Court's view, the interference with the applicant's right to respect for his private life had been necessary in the interests of national security and for the prevention of disorder and crime. However, the use of the information thus obtained in the context of a disciplinary investigation had not been in accordance with the law and the relevant legislation had been breached in two respects: the information had been used for purposes other than the one for which it had been gathered and had not been destroyed within the 15-day time-limit after the criminal investigation had ended. In this case the Court also found a **violation of Article 13** (right to an effective remedy) of the Convention, noting that in relation to both the criminal and disciplinary investigations the applicant had not had a domestic remedy available for securing a review of whether the interference was compatible with his right to respect for his private life and correspondence.

Figueiredo Teixeira v. Andorra

8 November 2016

This case concerned the storage and communication to the judicial authority of data from telephone calls made by the applicant, who was suspected of the serious offence of drug trafficking. The applicant complained in particular that the storage of data relating to his telephone communications had amounted to an unjustified interference with his right to respect for his private life.

The Court held that there had been **no violation of Article 8** of the Convention. It found in particular that since the impugned interference was prescribed in Andorran law under Article 87 of the Code of Criminal Procedure and Law No. 15/2003 on the protection of personal data, a person holding a prepaid mobile phone card could reasonably have expected those provisions to be applied in his case. Furthermore, the Court noted that Andorran criminal procedure provided a wide range of safeguards against arbitrary actions, given that a judge (a *batlle*) assessed the necessity and proportionality of the data transmission order in the light of the evidence gathered and the seriousness of the offence in question. The Court therefore found that, in the instant case, the balance between the applicant's right to respect for his private life and the prevention of criminal offences had been respected.

Dagregorio and Mosconi v. France

30 May 2017 (decision on the admissibility)

The applicants are two trade unionists who took part in the occupation and immobilisation of the *Société nationale Corse Méditerranée* (SNCM) ferry "Pascal Paoli" during the company takeover by a financial operator. The case concerned their refusal to undergo biological testing, the results of which were to be included in the national computerised DNA database (FNAEG). The applicants, having been convicted at first instance and on appeal, did not lodge an appeal on points of law.

The Court declared the application **inadmissible** for non-exhaustion of domestic remedies. It emphasised in particular that in the absence of any judicial precedent applicable to the applicants' situation, there was doubt as to the effectiveness of an appeal on points of law owing to a decision given by the Constitutional Council. The Court considered that it was therefore a point which should have been submitted to the Court of Cassation. The mere fact of harbouring doubts as to the prospects of a given appeal succeeding was not sufficient reason for omitting to use the remedy in question.

Aycaguer v. France

22 June 2017

The applicant alleged that there had been a breach of his right to respect for his private life on account of the order to provide a biological sample for inclusion in the national computerised DNA database (FNAEG) and the fact that his refusal to comply with that order had resulted in a criminal conviction.

The Court held that there had been a **violation of Article 8** of the Convention. It observed in particular that on 16 September 2010 the Constitutional Council had given a decision to the effect that the provisions on the FNAEG were in conformity with the Constitution, subject *inter alia* to "determining the duration of storage of such personal data depending on the purpose of the file stored and the nature and/or seriousness of the offences in question". The Court noted that, to date, no appropriate action had been taken on that reservation and that there was currently no provision for differentiating the period of storage depending on the nature and gravity of the offences committed. The Court also ruled that the regulations on the storage of DNA profiles in the FNAEG did not provide the data subjects with sufficient protection, owing to its duration and the fact that the data could not be deleted. The regulations therefore failed to strike a fair balance between the competing public and private interests.

Catt v. the United Kingdom

24 January 2019

This case concerned the complaint of the applicant, a lifelong activist, about the collection and retention of his personal data in a police database for "domestic extremists".

The Court held that there had been a **violation of Article 8** of the Convention. It found in particular that the data held on the applicant concerned his political views and that such information required particular protection. The Court also had regard to the applicant's age (94), and the fact he had no history or prospect of committing acts of violence. The Court further noted that, while collecting the information on him had been justified, retaining it had not, particularly owing to a lack of safeguards, such as time-limits.

Gaughran v. the United Kingdom

13 February 2020

This case concerned a complaint about the indefinite retention of personal data (DNA profile, fingerprints and photograph) of a man who had a spent conviction for driving with excess alcohol in Northern Ireland.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the United Kingdom had overstepped the acceptable margin of appreciation and the retention at issue constituted a disproportionate interference with the applicant's right to respect for private life, which could not be regarded as necessary in a democratic society. The Court underlined in particular that it was not the duration of the retention of data that had been decisive, but the absence of certain safeguards. In the applicant's case his personal data had been retained indefinitely without consideration of the seriousness of his offence, the need for indefinite retention and without any real possibility of review. Noting also that the technology being used had been shown to be more sophisticated than that considered by the domestic courts in this case, particularly regarding storage and analysis of photographs, the Court considered that the retention

of the applicant's data had failed to strike a fair balance between the competing public and private interests.

Algirdas Butkevičius v. Lithuania

14 June 2022

This case concerned a telephone conversation between the applicant – who, at the time, was the Prime Minister of Lithuania – and a mayor that was secretly recorded during a pre-trial investigation into possible corruption in connection with territorial planning and was made public at a hearing of the Lithuanian Parliament's (*Seima*'s) Anti-Corruption Commission. The applicant complained that the State authorities had breached his right to private life and correspondence by disclosing the telephone conversation to the media. He submitted in particular that the prosecutor and the Anti-Corruption Commission had not properly protected that information as they had been required to by law.

The Court held that there had been **no violation of Article 8** (right to respect for private life and correspondence) of the Convention in respect of the applicant, finding that, even if his reputation among his colleagues had been dinted by the disclosure of his telephone conversation, there were no factual grounds, let alone evidence, to indicate that it had been affected to a disproportionate degree. The Court noted in particular that the applicant had not pointed to any concrete and tangible repercussions which the media's disclosure of the telephone conversation had had on his private life, all the more so as he had not been convicted of anything and the Chief Official Ethics Commission had established nothing untoward in the conversation. It also reiterated the importance of public scrutiny in cases of possible political corruption.

Haščák v. Slovakia

23 June 2022

This case concerned a surveillance operation ("the Gorilla operation") carried out in 2005 and 2006 by the Slovak Intelligence Service (SIS) and the intelligence material obtained by it. The applicant – a prominent businessman associated with an influential finance group and a business partner of the applicant in the case of Zoltán Varga v. Slovakia (judgment of 20 July 2021) – complained, in particular, that there had been a lack of effective supervision and review of the implementation of two surveillance warrants issued by the Bratislava Regional Court in the mid-2000s, that the applicable framework provided no protection to individuals randomly affected by surveillance measures, and that the internal rules applicable to the retention of intelligence material were inadequate.

The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention concerning the implementation of the two warrants and the retention of the analytical material. It firstly stated that to a significant extent, the applicant's complaints under Article 8 were identical and arose from an identical factual and procedural background to that examined in the case of *Zoltán Varga*. It therefore applied that case-law to the present case. While there had been a basis in law, the Court observed in particular that the operation had had numerous deficiencies, some of which had been recognised at the domestic level in response to complaints and actions of Mr Varga. Although the domestic courts made no such findings in the individual case of the applicant, they were relevant to the assessment of his case. The Court reiterated that, as in *Zoltán Varga*, when implementing the surveillance warrants the SIS had practically enjoyed discretion amounting to unfettered power, which had not been accompanied by a measure of protection against arbitrary interference, as required by the rule of law. Furthermore, that situation had been aggravated by the uncontested fact that the applicant had not himself been the target of the surveillance under the first of the two warrants, in the light of his unchallenged argument that the law provided no protection to persons randomly affected by surveillance measures, and by the fundamental uncertainty around the practical and procedural status of the audio recording retrieved in 2018, presumably of SIS provenance. The Court lastly noted that it had previously held in *Zoltán Varga* that the storing of the analytical material obtained in the surveillance operation had been subject to confidential rules with no external

oversight. The retention had therefore not been in accordance with the law. The Court ruled that that also applied in the present case.

See also, among others:

Caruana v. Malta

15 May 2018 (decision on the admissibility)

P.N. v. Germany (no. 74440/17)

11 June 2020

In the context of health

Chave née Jullien v. France

9 July 1991 (decision of the European Commission of Human Rights[14])

This case concerned the storing in a psychiatric hospital records of information relating to the applicant's compulsory placement the illegality of which had been recognised by the French courts. The applicant considered in particular that the continued presence in a central record of information about her confinement in a psychiatric institution constituted an interference with her private life and wanted such information to be removed from central records of this type.

The Commission declared the application **inadmissible** as manifestly ill-founded. It observed in particular that the recording of information concerning mental patients served not just the legitimate interest of ensuring the efficient running of the public hospital service, but also that of protecting the rights of the patients themselves, especially in cases of compulsory placement. In the present case, the Commission noted, inter alia, that the information at issue was protected by appropriate confidentiality rules. In addition, these documents could not be equated with central records and were by no means accessible to the public, but only to exhaustively listed categories of persons from outside the institution. Therefore, the Commission found that the interference suffered by the applicant could not be held to have been disproportionate to the legitimate aim pursued, namely protection of health.

L.L. v. France (no. 7508/02)

10 October 2006

The applicant complained in particular about the submission to and use by the courts of documents from his medical records, in the context of divorce proceedings, without his consent and without a medical expert having been appointed in that connection.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the interference in the applicant's private life had not been justified in view of the fundamental importance of protecting personal data. It observed in particular that it was only on a subsidiary basis that the French courts had referred to the impugned medical report in support of their decisions, and it therefore appeared that they could have reached the same conclusion without it. The Court further noted that domestic law did not provide sufficient safeguards as regards the use in this type of proceedings of data concerning the parties' private lives, thus justifying a fortiori the need for a strict review as to the necessity of such measures.

Drelon v. France

8 September 2022

See above, under "Collection of personal data", "Data reflecting sexual orientation".

[14]. Together with the European Court of Human Rights and the Committee of Ministers of the Council of Europe, the European Commission of Human Rights, which sat in Strasbourg from July 1954 to October 1999, supervised Contracting States' compliance with their obligations under the European Convention on Human Rights. The Commission ceased to exist when the Court became permanent on 1st November 1998.

See also, recently:

Mockutė v. Lithuania
27 February 2018

In social insurance proceedings

Vukota-Bojić v. Switzerland
18 October 2016
The applicant had been involved in a road traffic accident, and subsequently requested a disability pension. Following a dispute with her insurer on the amount of disability pension and years of litigation later, her insurer requested that she undergo a fresh medical examination, in order to establish additional evidence about her condition. When she refused, the insurer hired private investigators to conduct secret surveillance of her. The evidence that they obtained was used in subsequent court proceedings, which resulted in a reduction of the applicant's benefits. She complained that the surveillance had been in breach of her right to respect for private life, and that it should not have been admitted in the proceedings.
The Court held that there had been a **violation of Article 8** of the Convention. It found in particular that the insurer's actions engaged state liability under the Convention, since the respondent insurance company was regarded as a public authority under Swiss law. It also held that the secret surveillance ordered had interfered with the applicant's private life, even though it had been carried out in public places, since the investigators had collected and stored data in a systematic way and had used it for a specific purpose. Furthermore, the surveillance had not been prescribed by law, since provisions of Swiss law on which it had been based were insufficiently precise. In particular, they had failed to regulate with clarity when and for how long surveillance could be conducted, and how data obtained by surveillance should be stored and accessed. The Court further found that the use of the surveillance evidence in the applicant's case against her insurer had not made the proceedings unfair and therefore held that there had been **no violation of Article 6** (right to a fair trial) of the Convention. In this respect it noted in particular that the applicant had been given a fair opportunity to challenge the evidence obtained by the surveillance, and that the Swiss court had given a reasoned decision as to why it should be admitted.

Mehmedovic v. Switzerland
11 December 2018 (decision on the admissibility)
This case concerned the surveillance of an insured person (the first applicant) and, indirectly, his wife, in public areas by investigators from an insurance company, with a view to ascertaining whether his claim for compensation, lodged following an accident, was justified.
The Court declared the application **inadmissible** as being manifestly ill-founded. In the first place, it noted that the insurance company's investigations, which had been conducted from a public place and were confined to ascertaining the first applicant's mobility, were aimed solely at protecting the insurer's pecuniary rights. In this connection, the Court held that the domestic courts had found that the insurer had an overriding interest that meant that the interference with the applicant's personality rights was lawful. Secondly, the Court noted that the sparse information concerning the second applicant, which had been gathered coincidentally and was of no relevance for the investigation, in no way constituted systematic or permanent gathering of data. In the Court's view, there had therefore been no interference with this applicant's private life.

Processing of sign-in data

Pending application

Le Marrec v. France (no. 52319/22)

Application communicated to the French Government on 7 March 2023

The applicant was in receipt of a social welfare allowance in the form of income support. In the course of processing his sign-in data the managing organisation (*Caisse d'allocations familiales* – Family Allowances Office) detected that he had submitted a quarterly statement of means from a foreign IP address. A review of his case was then undertaken. On completion of the review his entitlement to the allowance was withdrawn with retroactive effect. The applicant's complaint concerns the processing of his sign-in data (in particular the geolocation of his IP address), which he argues was not subject to adequate legal safeguards, and the domestic courts' failure to address the privacy ground which he had raised in that regard.

The Court gave notice of the application to the French Government and put questions to the parties under Article 8 (right to respect for private life) Article 6 § 1 (right to a fair trial) of the Convention.

Storage in secret registers

Leander v. Sweden

23 March 1987

This case concerned the use of a secret police file in the recruitment of a carpenter. The applicant, who had been working as a temporary replacement at the Naval Museum in Karlskrona, next to a restricted military security zone, complained about the storage of data related to his trade-union activities a long time before and alleged that this had led to his exclusion from the employment in question. He contended that nothing in his personal or political background could be regarded as of such a nature as to make it necessary to register him in the Security Department's register and to classify him as a "security risk".

The Court held that there had been **no violation of Article 8** of the Convention. Noting in particular that both the storing in a secret register and the release of information about an individual's private life fell within the scope of Article 8 of the Convention, the Court also recalled that, in a democratic society, the existence of intelligence services and the storage of data could be lawful and prevail over the interest of citizens provided that it pursued legitimate aims, namely the prevention of disorder or crime or the protection of national security. In this case, the Court found that the safeguards contained in the Swedish personnel-control system satisfied the requirements of Article 8 of the Convention and that the Swedish Government had been entitled to consider that the interests of national security prevailed over the applicant's individual interests.

Rotaru v. Romania

4 May 2000 (Grand Chamber)

See below, under "Erasure or destruction of personal data".

Turek v. Slovakia

14 February 2006

See below under "Access to personal data".

Tax information

L.B. v. Hungary (no. 36345/16)

9 March 2023 (Grand Chamber)

This case concerned the Hungarian legislative policy of publishing the personal data of taxpayers who were in debt. The applicant complained in particular that his name and

home address had been published on a list of "major tax debtors" on the tax authorities' website under a 2006 amendment to the relevant tax legislation.
The Court held that there had been a **violation of Article 8** of the Convention. It found in particular that the amended publication scheme had been systematic, without any weighing up of the public interest in ensuring tax discipline against the individual's privacy rights. Also, Parliament had not assessed the previous publication schemes and their impact on taxpayers or reflected as to what the additional value would be of the 2006 amended scheme. Moreover, little or no consideration had been given to data protection, the risk of misuse by the general public of a tax debtor's home address, or the worldwide reach of Internet. The Court was not therefore satisfied, notwithstanding the respondent State's wide discretion to decide on such matters, that the Hungarian legislature's reasons for enacting the amended publication scheme, although relevant, had been sufficient to show that the interference with the applicant's rights had been "necessary in a democratic society".

Pending application

Casarini v. Italy (no. 25578/11)

Application communicated to the Italian Government on 8 February 2021
This case concerns the alleged absence of sufficient safeguards against abuse of access to personal data stored in the database of the Taxpayers Information Service (*Servizio per le informazioni sul contribuente – Ser.P.I.Co.*).
The Court gave notice of the application to the Italian Government and put questions to the parties under Article 8 and Article 35 (admissibility criteria) of the Convention.

Telecommunication service providers' data

Breyer v. Germany

30 January 2020
In accordance with 2004 amendments to the German 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. They complained about the storage of their personal data as users of pre-paid SIM cards.
The Court held that there had been **no violation of Article 8** of the Convention, finding that, overall, Germany had not overstepped the limits of its discretion ("margin of appreciation") it had in applying the law concerned, when choosing the means to achieve the legitimate aims of protecting national security and fighting crime, and 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. The Court considered 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. It noted, however, that 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.

Disclosure of personal data

Z. v. Finland (no. 22009/93)

25 February 1997
This case concerned the disclosure of the applicant's condition as HIV-positive in criminal proceedings against her husband.
The Court held that there had been a **violation of Article 8** of the Convention, finding that the disclosure of the applicant's identity and HIV infection in the text of the Court of

Appeal's judgment made available to the press was not supported by any cogent reasons and that the publication of the information concerned had accordingly given rise to a violation of the applicant's right to respect for her private and family life. The Court noted in particular that respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention and is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention.

M.S. v. Sweden (no. 20837/92)

27 August 1997

This case concerned the communication by a clinic to a social-security body of medical records containing information about an abortion performed on the applicant.

The Court held that there had been **no violation of Article 8** of the Convention, finding that there had been relevant and sufficient reasons for the communication of the applicant's medical records by the clinic to the social-security body and that the measure had not been disproportionate to the legitimate aim pursued, namely, by enabling the social-security body to determine whether the conditions for granting the applicant compensation for industrial injury had been met, to protect the economic well-being of the country. Moreover, the contested measure was subject to important limitations and was accompanied by effective and adequate safeguards against abuse.

Peck v. the United Kingdom

28 January 2003

This case concerned the disclosure to the media of footage filmed in a street by a closed-circuit television (CCTV) camera installed by the local council, showing the applicant cutting his wrists.

The Court found that the disclosure of the footage by the Municipal Council had not been accompanied by sufficient safeguards and constituted disproportionate and unjustified interference with the applicant's private life, **in breach of Article 8** of the Convention. It did in particular not find that, in the circumstances of this case, there were relevant or sufficient reasons which would justify the direct disclosure by the Council to the public of stills from the footage without the Council obtaining the applicant's consent or masking his identity, or which would justify its disclosures to the media without the Council taking steps to ensure so far as possible that such masking would be effected by the media. The crime-prevention objective and context of the disclosures demanded particular scrutiny and care in these respects in the present case. The Court also held that there had been a **violation of Article 13** (right to an effective remedy) of the Convention **read in conjunction with Article 8**, finding that the applicant had had no effective remedy in relation to the violation of his right to respect for his private life.

Panteleyenko v. Ukraine

29 June 2006

The applicant complained in particular about the disclosure at a court hearing of confidential information regarding his mental state and psychiatric treatment.

The Court found that obtaining from a psychiatric hospital confidential information regarding the applicant's mental state and relevant medical treatment and disclosing it at a public hearing had constituted an interference with the applicant's right to respect for his private life. It held that there had been a **violation of Article 8** of the Convention, noting in particular that the details in issue were incapable of affecting the outcome of the litigation, that the first-instance court's request for information was redundant, as the information was not "important for an inquiry, pre-trial investigation or trial", and was thus unlawful for the purposes of the Psychiatric Medical Assistance Act 2000.

Armonas v. Lithuania and Biriuk v. Lithuania

25 November 2008

In 2001, Lithuania's biggest daily newspaper published an article on its front page concerning an AIDS threat in a remote part of Lithuania. In particular, medical staff from an AIDS centre and an hospital were cited as having confirmed that the applicants were HIV positive. The second applicant, described as "notoriously promiscuous", was also said to have had two illegitimate children with the first applicant.

The Court held that there had been a **violation of Article 8** of the Convention on account of the low ceiling imposed on damages awarded to the applicants. Particularly concerned about the fact that, according to the newspaper, the information about the applicants' illness had been confirmed by medical staff, it observed that it was crucial that domestic law safeguarded patient confidentiality and discouraged any disclosures on personal data, especially bearing in mind the negative impact of such disclosures on the willingness of others to take voluntary tests for HIV and seek appropriate treatment.

Avilkina and Others v. Russia[15]

6 June 2013

The applicants were a religious organisation, the Administrative Centre of Jehovah's Witnesses in Russia, and three Jehovah's Witnesses. They complained in particular about the disclosure of their medical files to the Russian prosecution authorities following their refusal to have blood transfusions during their stay in public hospitals. In connection with an inquiry into the lawfulness of the applicant organisation's activities, the prosecuting authorities had instructed all St. Petersburg hospitals to report refusals of blood transfusions by Jehovah's Witnesses.

The Court declared the application **inadmissible** (incompatible *ratione personae*) as regards the applicant religious organisation, and as regards one of the three other applicants, as no disclosure of her medical files had actually taken place, and this was not in dispute by the parties. The Court further held that there had been a **violation of Article 8** of the Convention as concerned the two other applicants. It notably found that there had been no pressing social need to disclose confidential medical information on them. Furthermore, the means employed by the prosecutor in conducting the inquiry, involving disclosure of confidential information without any prior warning or opportunity to object, need not have been so oppressive for the applicants. Therefore the authorities had made no effort to strike a fair balance between, on the one hand, the applicants' right to respect for their private life and, on the other, the prosecutor's aim of protecting public health.

See also: **Y.Y. v. Russia (no. 40378/06)**, judgment of 23 February 2016[16].

Radu v. the Republic of Moldova

15 April 2014

The applicant, a lecturer at the Police Academy, complained about a State-owned hospital's disclosure of medical information about her to her employer. The information was widely circulated at the applicant's place of work and, shortly afterwards, she had a miscarriage due to stress. She unsuccessfully brought proceedings against the hospital and the Police Academy.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the interference with the exercise of the right to respect for private life complained of by the applicant was not "in accordance with the law" within the meaning of Article 8.

Sõro v. Estonia

3 September 2015

This case concerned the applicant's complaint about the fact that information about his employment during the Soviet era as a driver for the Committee for State Security of the USSR (the KGB) had been published in the Estonian State Gazette in 2004.

[15]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.
[16]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

The Court held that there had been **violation of Article 8** of the Convention, finding that in the applicant's case this measure had been disproportionate to the aims sought. The Court noted in particular that, under the relevant national legislation, information about all employees of the former security services – including drivers, as in the applicant's case – was published, regardless of the specific function they had performed. Furthermore, while the Disclosure Act had come into force three and a half years after Estonia had declared its independence, publication of information about former employees of the security services had stretched over several years. In the applicant's case, the information in question had only been published in 2004, almost 13 years after Estonia had declared its independence, and there had been no assessment of the possible threat posed by the applicant at the time the announcement was published. Finally, although the Disclosure Act itself did not impose any restrictions on the applicant's employment, according to his submissions he had been derided by his colleagues and had been forced to quit his job. The Court considered that even if such a result was not sought by the Act it nevertheless testified to how serious the interference with the applicant's right to respect for his private life had been.

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland

27 June 2017 (Grand Chamber)

After two companies had published the personal tax information of 1.2 million people, the domestic authorities ruled that such wholesale publication of personal data had been unlawful under data protection laws, and barred such mass publications in future. The companies complained that the ban had violated their right to freedom of expression.

The Grand Chamber held, by fifteen votes to two, that there had been **no violation of Article 10** (freedom of expression) of the Convention. It noted in particular that the ban had interfered with the companies' freedom of expression. However, it had not violated Article 10 because it had been in accordance with the law, it had pursued the legitimate aim of protecting individuals' privacy, and it had struck a fair balance between the right to privacy and the right to freedom of expression. In this case, the Grand Chamber agreed with the conclusion of the domestic courts, that the mass collection and wholesale dissemination of taxation data had not contributed to a debate of public interest, and had not been for a solely journalistic purpose.

See also: **Samoylova v. Russia**, judgment of 14 December 2021[17].

Standard Verlagsgesellschaft mbH v. Austria (No. 3)

7 December 2021

This case concerned court orders for the applicant media company to reveal the sign-up information of registered users who had posted comments on its website, derStandard.at, the website of the newspaper *Der Standard*. This had followed comments allegedly linking politicians to, among other things, corruption or neo-Nazis, which the applicant company had removed, albeit refusing to reveal the information of the commenters.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention in the present case, finding that the court orders in question had not been necessary in a democratic society. The Court found, in particular, that user data did not enjoy the protection of "journalistic sources", and there was no absolute right to online anonymity. However, the domestic courts had not even balanced the interests of the plaintiffs with the interests of the applicant company in keeping its users anonymous so as to help promote the free exchange of ideas and information as covered by Article 10 of the Convention.

[17]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

Y.G. v. Russia (no. 8647/12)[18]

30 August 2022

This case concerned the collection of health data, including that of the applicant, who was HIV-positive and suffered from hepatitis, in a database that was made available for sale at a market. The applicant submitted that the law-enforcement authorities had unlawfully collected, stored and entered his health data in a database, and that they had failed to ensure the confidentiality of his data and to carry out an effective investigation into their disclosure.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the Russian authorities had failed to comply with their positive obligation to ensure adequate protection of the applicant's right to respect for his private life. It noted in particular that it was uncontested that only the authorities had access to most of the data on the database, such as criminal records and preventive measures that had been applied, and that, in the past, in the context of criminal proceedings against the applicant, the investigator in charge had sought information about the applicant's health condition from the Hospital for Infectious Diseases. Although it was in dispute whether the Ministry of the Interior had compiled the database, in the context of the case, there was no explanation other than that the State authorities, who had access to the data in question, had failed to prevent a breach of confidentiality. As a result, that data had become publicly available, thus engaging the responsibility of the respondent State. The circumstances of this major privacy breach had never been elucidated. The Court recalled in that respect that it had repeatedly stressed the importance of appropriate safeguards to prevent the communication and disclosure of health data.

Access to personal data

Gaskin v. the United Kingdom

7 July 1989

On reaching the age of majority the applicant, who had been taken into care as a child, wished to find out about his past in order to overcome his personal problems. He was refused access to his file on the ground that it contained confidential information.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the procedures followed had failed to secure respect for the applicant's private and family life as required by that Article. It noted in particular that persons in the situation of the applicant had a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which made access to records dependent on the consent of the contributor, could in principle be considered to be compatible with the obligations under Article 8, taking into account the State's margin of appreciation. The Court considered, however, that under such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case.

Odièvre v. France

13 February 2003 (Grand Chamber)

The applicant was abandoned by her natural mother at birth and left with the Health and

[18]. On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

Social Security Department. She complained that she had been unable to obtain details identifying her natural family and said in particular that her inability to do so was highly damaging to her as it deprived her of the chance of reconstituting her life history.
In its Grand Chamber judgment, the Court noted that birth, and in particular the circumstances in which a child was born, formed part of a child's, and subsequently the adult's, private life guaranteed by Article 8 of the Convention. In the instant case, it held that there had been **no violation of Article 8**, observing in particular that the applicant had been given access to non-identifying information about her mother and natural family that enabled her to trace some of her roots, while ensuring the protection of third-party interests. In addition, recent legislation enacted in 2002 enabled confidentiality to be waived and set up a special body to facilitate searches for information about biological origins. The applicant could now use that legislation to request disclosure of her mother's identity, subject to the latter's consent being obtained to ensure that the mother's need for protection and the applicant's legitimate request were fairly reconciled. The French legislation thus sought to strike a balance and to ensure sufficient proportion between the competing interests.

Roche v. the United Kingdom

19 October 2005 (Grand Chamber)
The applicant was discharged from the British Army in the late 1960s. In the 1980s he developed high blood pressure and later suffered from hypertension, bronchitis and bronchial asthma. He was registered as an invalid and maintained that his health problems were the result of his participation in mustard and nerve gas tests conducted under the auspices of the British Armed Forces at Porton Down Barracks (England) in the 1960s. The applicant complained in particular that he had not had access to all relevant and appropriate information that would have allowed him to assess any risk to which he had been exposed during his participation in those tests.
The Court held that there had been a **violation of Article 8** of the Convention, finding that, in the overall circumstances, the United Kingdom had not fulfilled its positive obligation to provide an effective and accessible procedure enabling the applicant to have access to all relevant and appropriate information which would allow him to assess any risk to which he had been exposed during his participation in the tests. The Court observed in particular that an individual, such as the applicant, who had consistently pursued such disclosure independently of any litigation, should not be required to litigate to obtain disclosure. In addition, information services and health studies had only been started almost 10 years after the applicant had begun his search for records and after he had lodged his application with the Court.

Turek v. Slovakia

14 February 2006
The applicant alleged in particular that the continued existence of a former Czechoslovak Communist Security Agency file registering him as one of its agents, the issuance of a security clearance to that effect, the dismissal of his action challenging that registration and the resultant effects constituted a violation of his right to respect for his private life.
The Court recognised that, particularly in proceedings related to the operations of state security agencies, there might be legitimate grounds to limit access to certain documents and other materials. However, in respect of lustration proceedings, that consideration lost much of its validity, particularly since such proceedings were by their nature orientated towards the establishment of facts dating from the communist era and were not directly linked to the current functions of the security services. Furthermore, it was the legality of the agency's actions which was in question. In the applicant's case, it noted that the domestic courts had considered it of crucial importance for him to prove that the State's interference with his rights was contrary to the applicable rules. Those rules were, however, secret and the applicant did not have full access to them. On the other hand, the State – the Slovak Intelligence Service – did have full access. The Court found that that requirement placed an unrealistic and excessive burden on the applicant and did not respect the principle of equality. There had therefore been a **violation of**

Article 8 of the Convention concerning the lack of a procedure by which the applicant could seek protection for his right to respect for his private life. The Court lastly found it unnecessary to examine separately the effects on the applicant's private life of his registration in the former State Security Agency files and of his negative security clearance.

Segerstedt-Wiberg and Others v. Sweden

6 June 2006

In this case the applicants were denied access to the full files held on them by the Swedish Security Police, on the grounds that to give them access might compromise the prevention of crime or the protection of national security.

The Court held that there had been **no violation of Article 8** of the Convention on account of the refusal to grant the applicants full access to information stored about them by the Security Police. Reiterating in particular that a refusal of full access to a national secret police register was necessary where the State might legitimately fear that the provision of such information might jeopardise the efficacy of a secret surveillance system designed to protect national security and to combat terrorism, the Court found that Sweden, having regard to the wide margin of appreciation available to it, was entitled to consider that the interests of national security and the fight against terrorism prevailed over the interests of the applicants in being advised of the full extent to which information was kept about them on the Security Police register.

K.H. and Others v. Slovakia (no. 32881/04)

28 April 2009

The applicants, eight women of Roma origin, could not conceive any longer after being treated at gynaecological departments in two different hospitals, and suspected that it was because they had been sterilised during their stay in those hospitals. They complained that they could not obtain photocopies of their medical records.

The Court held that there had been a **violation of Article 8** of the Convention in that the applicants had not been allowed to photocopy their medical records. It considered in particular that persons who, like the applicants, wished to obtain photocopies of documents containing their personal data, should not have been obliged to make specific justification as to why they needed the copies. It should have been rather for the authority in possession of the data to show that there had been compelling reasons for not providing that facility. Given that the applicants had obtained judicial orders permitting them to consult their medical records in their entirety, having denied them the possibility to make photocopies of those records had not been sufficiently justified by the authorities. To avoid the risk of abuse of medical data it would have been sufficient to put in place legislative safeguards with a view to strictly limiting the circumstances under which such data could be disclosed, as well as the scope of persons entitled to have access to the files. The Court observed that the new Health Care Act adopted in 2004 had been compatible with that requirement, however, it had come into play too late to affect the situation of the applicants in this case.

Haralambie v. Romania

27 October 2009

The applicant complained in particular about the obstacles to his right of access to the personal file created on him by the former secret services during the communist period.

The Court held that there had been a **violation of Article 8** of the Convention, on account of the obstacles to the applicant's consultation of the personal file created on him by the secret service under the communist regime. It found that neither the quantity of files transferred nor shortcomings in the archive system justified a delay of six years in granting his request. In this case the Court reiterated in particular the vital interest for individuals who were the subject of personal files held by the public authorities to be able to have access to them and emphasised that the authorities had a duty to provide an effective procedure for obtaining access to such information.

See also: **Jarnea v. Romania**, judgment of 19 July 2011; **Antoneta Tudor v.**

Romania, judgment of 24 September 2013.

Godelli v. Italy

25 September 2012

This case concerned the confidentiality of information concerning a child's birth and the inability of a person abandoned by her mother to find out about her origins. The applicant maintained that she had suffered severe damage as a result of not knowing her personal history, having been unable to trace any of her roots while ensuring the protection of third-party interests.

The Court held that there had been a **violation of Article 8** of the Convention, considering in particular that a fair balance had not been struck between the interests at stake since the Italian legislation, in cases where the mother had opted not to disclose her identity, did not allow a child who had not been formally recognised at birth and was subsequently adopted to request either non-identifying information about his or her origins or the disclosure of the birth mother's identity with the latter's consent.

Magyar Helsinki Bizottság v. Hungary

8 November 2016 (Grand Chamber)

This case concerned the authorities' refusal to provide an NGO with information relating to the work of *ex officio* defence counsel, as the authorities had classified that information as personal data that was not subject to disclosure under Hungarian law. The applicant NGO complained that the Hungarian courts' refusal to order the surrender of the information in question had amounted to a breach of its right to access to information.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It observed in particular that the information requested by the applicant NGO was necessary for it to complete the study on the functioning of the public defenders' system being conducted by it in its capacity as a non-governmental human-rights organisation, with a view to contributing to discussion on an issue of obvious public interest. In the Court's view, by denying the applicant NGO access to the requested information the domestic authorities had impaired the NGO's exercise of its freedom to receive and impart information, in a manner striking at the very substance of its Article 10 rights. The Court further noted that the public defenders' privacy rights would not have been negatively affected had the applicant NGO's request for the information been granted, because although the information request had admittedly concerned personal data, it did not involve information outside the public domain. The Court also found that the Hungarian law, as interpreted by the domestic courts, had excluded any meaningful assessment of the applicant NGO's freedom-of-expression rights, and considered that in the present case, any restrictions on the applicant NGO's proposed publication – which was intended to contribute to a debate on a matter of general interest – ought to have been subjected to the utmost scrutiny. Lastly, the Court considered that the Hungarian Government's arguments were not sufficient to show that the interference complained of had been "necessary in a democratic society" and held that, notwithstanding the discretion left to the respondent State (its "margin of appreciation"), there had not been a reasonable relationship of proportionality between the measure complained of (refusal to provide the names of the *ex officio* defence counsel and the number of times they had been appointed to act as counsel in certain jurisdictions) and the legitimate aim pursued (protection of the rights of others).

See also, among others: **Centre for Democracy and the Rule of Law v. Ukraine**, decision on the admissibility of 3 March 2020; **Centre for Democracy and the Rule of Law v. Ukraine**, judgment of 26 March 2020; **Saure v. Germany**, decision on the admissibility of 19 October 2021; **Mitov and Others v. Bulgaria**, decision on the admissibility of 28 February 2023.

Erasure or destruction of personal data

Rotaru v. Romania

4 May 2000 (Grand Chamber)

The applicant complained that it was impossible to refute what he claimed was untrue information in a file on him kept by the Romanian Intelligence Service (RIS). He had been sentenced to a year's imprisonment in 1948 for having expressed criticism of the communist regime.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the holding and use by the RIS of information about the applicant's private life had not been in accordance with the law. The Court observed in particular that public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past. It further noted that no provision of domestic law defined the kind of information that could be recorded, the categories of people against whom surveillance measures such as gathering and keeping information could be taken, the circumstances in which such measures could be taken or the procedure to be followed. Similarly, the law did not lay down limits on the age of information held or the length of time for which it could be kept. Lastly, there existed no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that could be made of the information thus obtained. That being so, the Court considered that Romanian law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. In this case there Court also held that there had been a **violation of Article 13** (right to an effective remedy) of the Convention because it was impossible for the applicant to challenge the data storage or to refute the truth of the information in question.

See also: **Association "21 December 1989" and Others v. Romania**, judgment of 24 May 2011.

Further reading

See in particular:

- **Council of Europe Convention (no. 108) for the Protection of Individuals with regard to Automatic Processing of Personal Data**, adopted in Strasbourg on 28 January 1981
- Council of Europe **web page** on data protection
- **Handbook on European Data Protection Law**, European Union Agency for Fundamental Rights / Council of Europe, 2014

Media Contact:
Tel.: +33 3 90 21 42 08