June 2016
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 Court 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

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.

[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."

Pending application

Ben Faiza v. France (application no. 31446/12)

Application communicated to the French Government on 3 February 2015

The applicant in this case complains in particular of an interference with his private life on account of the installation of a GPS tracking device in his vehicle with the aim of monitoring his movements during the course of a drug trafficking inquiry.

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) of the Convention.

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.

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 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.

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[2] and "appropriate adults"[3].

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

4 December 2015

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.

[2] A juvenile or person who is mentally disordered or otherwise mentally vulnerable

[3] An "appropriate adult" could be a relative or guardian, or a person experienced in dealing with mentally disordered or mentally vulnerable people.

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.

Pending applications

Centrum För Rättvisa v. Sweden (no. 35252/08)

Application communicated to the Swedish Government on 21 November 2011 and 14 October 2014

The applicant, a non-profit public interest law firm, complains about the Swedish state practice and legislation concerning secret surveillance measures.

The Court gave notice of the application to the Swedish Government and put questions to the parties under Articles 8 (right to respect for private life), 13 (right to an effective remedy) and 34 (individual applications) of the Convention.

Tretter and Others v. Austria (no. 3599/10)

Application communicated to the Austrian Government on 6 May 2013

This case concerns the amendments of the Police Powers Act, which entered into force in January 2008 and extended the powers of the police authorities to collect and process personal data.

The Court communicated the application to the Austrian Government and put questions to the parties under Articles 34 (right of individual petition), 8 (right to respect for private and family life and correspondence) and 10 (freedom of expression) of the Convention.

Big Brother Watch and Others v. the United Kingdom (no. 58170/13)

Application communicated to the UK Government on 9 January 2014

The applicants, three NGOs and one academic working internationally in the fields of privacy and freedom of expression, allege they are likely to have been the subjects of surveillance by the United Kingdom intelligence services. Their concerns have been triggered by media coverage following the revelations by Edward Snowden, a former systems administrator with the United States National Security Agency (the NSA).

The Court gave notice of the application to the UK Government and put questions to the parties under Article 8 (right to respect for private life) of the Convention.

Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14)

Application communicated to the UK Government on 5 January 2015

This case concerns the allegations of the applicants – the Bureau of Investigative Journalism and an investigative reporter who has worked for the Bureau – regarding the interception of both internet and telephone communications by government agencies in the United Kingdom, and, in particular, by the Government Communication Headquarters (GCHQ), as revealed by Edward Snowden, a former systems administrator with the United States National Security Agency (the NSA). The applicants mainly complain that the blanket interception, storage and exploitation of communication amount to disproportionate interference with journalistic freedom of expression.

The Court gave notice of the application to the UK Government and put questions to the parties under Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.

Similar application pending:

10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15)

Application communicated to the UK Government on 24 November 2015

The Court gave notice of the application to the UK Government and put questions to the parties under Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life), 10 (freedom of expression), 14 (prohibition of discrimination) and 34 (individual applications) of the Convention.

Monitoring of employees' computer use

Pending applications

Bărbulescu v. Romania

12 January 2016 (Chamber judgment) – case referred to the Grand Chamber in June 2016

This case concerns the applicant's dismissal by his employer, a private company, for having used the company's Internet for personal purposes during working hours in breach of internal regulations. The applicant complains in particular that his employer's decision to terminate his contract was based on a breach of his privacy.

In its Chamber judgment of 12 January 2016 the Court held, by six votes to one, that there had been **no violation of Article 8** (right to respect for private and family life, the home and correspondence) of the Convention, finding that the domestic courts had struck a fair balance between the applicant's right to respect for his private life and correspondence under Article 8 and the interests of his employer. The Chamber observed, in particular, that the applicant's private life and correspondence had been engaged. However his employer's monitoring of his communications had been reasonable in the context of disciplinary proceedings.

On 6 June 2016 the Grand Chamber Panel accepted the applicant's request that the case be referred to the Grand Chamber.

Libert v. France (no. 588/13)

Application communicated to the French Government on 30 March 2015

The applicant complains in particular of a violation of his right to respect for his private life arising from the fact that his employer (The French national rail company, SNCF) opened files on his professional computer's hard drive named « D:/personal data » without him being present. He was later struck off because of the contents of the files in question.

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) of the Convention.

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.

Pending application

Antović and Mirković v. Montenegro (no. 70838/13)

Application communicated to the Montenegrin Government on 3 December 2014

This case concerns the use of video surveillance in university classrooms, which the applicants – two university professors – claim violates domestic data protection law.

The Court gave notice of the application to the Montenegrin Government and put questions to the parties under Articles 8 (right to respect for private and family life) and 35 (admissibility criteria) of the Convention.

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)

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.

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[4] 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.

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

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.

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

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 break up 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 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.

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**, 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.

Pending applications

Dagregorio and Mosconi v. France (no. 65714/11) and Aycaguer v. France (no. 8806/12)

Applications communicated to the French Government on 26 March 2014

The applicants complain in particular about their conviction for refusing to undergo biological testing for the purposes of identifying their DNA. The data collected were to have been entered into the FNAEG automated DNA database (*Fichier national automatisé des empreintes génétiques*).

The Court gave notice of the applications to the French Government and put questions to the parties under Article 8 (right to respect for private life) of the Convention as well as, in the case of *Dagregorio and Mosconi*, under Article 14 (prohibition of discrimination) of the Convention.

López Ribalda v. Spain (no. 1874/13) and Gancedo Giménez and Others v. Spain (no. 8567/13)

Applications communicated to the Spanish Government on 17 February 2015

This case concerns the use of video surveillance in the workplace, which was then used as evidence in national courts.

The Court gave notice of the applications to the Spanish Government and put questions to the parties Articles 6 (right to a fair trial) and 8 (right to respect for private and family life) of the Convention.

In the contexte of health

Chave née Jullien v. France

9 July 1991 (decision of the European Commission of Human Rights[5])

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 psychiatiic 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** (right to respect for private and family life) 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.

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

[5]. 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.

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.

Telecommunication service providers' data

Pending applications

Breyer v. Germany (no. 50001/12)

Application communicated to the German Government on 21 March 2016
The application concerns the legal obligation of telecommunication providers to store personal details of all their customers.
The Court gave notice of the application to the German Government and put questions to the parties under Articles 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.

Ćalović v. Montenegro (no. 18667/11)

Application communicated to the Government of Montenegro on 31 March 2016
The applicant complains about the powers of the police to access directly all data of the mobile telecommunication provider to which she is subscribed, therefore including her own, in an uncontrolled manner.
The Court gave notice of the application to the Government of Montenegro and put questions to the parties under Articles 8 (right to respect for private life), 34 (individual applications) and 35 (admissibility criteria) of the Convention.

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** (right to respect for private and family life) 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

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: ***Radu v. the Republic of Moldova***, judgment of 15 April 2014; ***Y.Y. v. Russia (no. 40378/06)***, judgment of 23 February 2016.

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.

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.

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 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** (right to respect for private life), 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.

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.

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 furher 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 May2011.

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