February 2020
This Factsheet does not bind the Court and is not exhaustive

New technologies

Electronic data

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[1] after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case.

The European Court of Human Right held that there had been a **violation of Article 8** (right to respect for private life) of the European Convention on Human Rights. It 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 (application no. 5335/06), Gardel v. France and M.B. v. France (no. 22115/06)

17 December 2009

The three applicants – convicted of rape of 15 year-old minors by a person in a position of authority – complained, in particular, about their inclusion in the national Sex Offender Database.

The Court held that there had been **no violation of Article 8** (right to respect for private life) of the Convention. It took the view that the length of the data conservation – 30 years maximum – was not disproportionate in relation to the aim pursued – prevention of crime – by the retention of the information. Moreover, 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.

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** (right to respect for private life) of the Convention. It observed 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

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

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. The Court also held that there had been a **violation of Article 5** (right to liberty and security) of the Convention.

Mandil v. France, Barreau and Others v. France and Deceuninck v. France

13 November 2011 (decisions on the admissibility)

The applicants were "Faucheurs volontaires" (Volunteer Reapers) who had participated in digging up experimental crops of transgenic beetroot. The applicant in the first case complained about his conviction for refusing to provide a biological sample to be stored on the national computerised DNA database; the applicants in the second case argued that the storage of their DNA on the national computerised database and the conviction of a number of them for refusing to provide a biological sample amounted to a violation of their right to respect for private life; the applicant in the third case submitted in particular that the order to take cell samples containing his genetic information constituted a disproportionate interference with his integrity and his private life.

The Court declared the applications **inadmissible** for failure to respect duty of confidentiality in friendly settlement negotiations. It considered that the applicants had violated the principle of confidentiality enshrined in Article 39 § 2 of the Convention and Rule 62 of the Rules of Court and that their conduct had constituted a violation of the right of individual petition for the purposes of Article 35 § 3 (a) of the Convention.

Robathin v. Austria

3 July 2012

A practising lawyer, the applicant complained about a search carried out in his office in 2006 and seizure of documents as well as all his electronic data following criminal proceedings brought against him on suspicion of theft, embezzlement and fraud of his clients. He was ultimately acquitted of all charges against him in 2011.

The Court held that there had been a **violation of Article 8** (right to respect for correspondence) of the Convention. It observed in particular that, although the applicant had benefited from a number of procedural safeguards, the review chamber to which he had referred the case had given only brief and rather general reasons when authorising the search of all the electronic data from the applicant's law office, rather than data relating solely to the relationship between the applicant and the victims of his alleged offences. In view of the specific circumstances prevailing in a law office, particular reasons should have been given to allow such an all-encompassing search. In the absence of such reasons, the Court found that the seizure and examination of all the data had gone beyond what was necessary to achieve the legitimate aim.

Bernh Larsen Holding As and Others v. Norway

14 March 2013

This case concerned the complaint by three Norwegian companies about a decision of the tax authorities ordering tax auditors to be provided with a copy of all data on a computer server used jointly by the three companies. The applicant companies alleged in particular that the measure in question had been taken in an arbitrary manner.

The Court held that there had been **no violation of Article 8** (right to respect for home and correspondence) of the Convention. It agreed with the Norwegian courts' argument that, for efficiency reasons, tax authorities' possibilities to act should not be limited by the fact that a tax payer was using a "mixed archive", even if that archive contained data belonging to other tax payers. Moreover, there were adequate safeguards against abuse.

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

18 April 2013

The applicant, who had been the subject of two investigations concerning book theft, which ended in one case with his acquittal and in the other with a decision not to

prosecute, complained of the fact that his fingerprints had been retained on a database by the French authorities.
The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention. It considered, in view of the circumstances of the case, that the retention of the data in question had amounted to disproportionate interference with the applicant's right to respect for his private life.

Youth Initiative For Human Rights v. Serbia

25 June 2013
This case concerned access to information obtained via electronic surveillance by the Serbian Intelligence Agency. The applicant NGO complained that the intelligence agency's refusal to provide it with the information it had requested – it had requested to be provided with information on how many people the agency had subjected to electronic surveillance in 2005 – prevented it from exercising its role as "public watchdog".
The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It found that the agency's obstinate reluctance to comply with a final and binding order to provide information it had obtained was in defiance of domestic law and was tantamount to being arbitrary.
Under Article 46 (binding force and implementation) of the Convention, the Court further held that the most natural way to implement its judgment in this case would be to ensure that the agency provided the applicant NGO with the information it had requested on how many people had been subjected to electronic surveillance in 2005.

Nagla v. Latvia

16 July 2013
This case concerned the search by the police of a well-known broadcast journalist's home, and their seizure of data storage devices. The applicant's home was searched following a broadcast she had aired in February 2010 informing the public of an information leak from the State Revenue Service database. The applicant complained that the search of her home meant that she had been compelled to disclose information that had enabled a journalistic source to be identified, violating her right to receive and impart information.
The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It emphasised that the right of journalist's not to disclose their sources could not be considered a privilege, dependent on the lawfulness or unlawfulness of their sources, but rather as an intrinsic part of the right to information that should be treated with the utmost caution. In this case the investigating authorities had failed to properly balance the interest of the investigation in securing evidence against the public interest in protecting the journalist's freedom of expression.

Peruzzo and Martens v. Germany

4 June 2013 (decision on the admissibility)
The applicants, who had been convicted of serious criminal offences, complained under Article 8 (right to respect for private life) of the Convention 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 being manifestly ill-founded. The measures complained of were found to constitute a proportionate interference with the applicants' right to respect for their private life and were necessary in a democratic society.

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** (right to respect for private life) 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.

Sérvulo & Associados - Sociedade de Advogados, RL v. Portugal

3 September 2015
This case concerned the search of a law firm's offices and the seizure of computer files and email messages, during an investigation into suspected corruption, acquisition of prohibited interests and money laundering in connection with the purchase by the Portuguese Government of two submarines from a German consortium.
The Court held that there had been **no violation of Article 8** (right to respect for private life and correspondence) of the Convention. It found that, notwithstanding the scope of the search and seizure warrants, the safeguards afforded to the applicants against abuse, arbitrariness and breaches of legal professional secrecy had been adequate and sufficient. Hence, the search and seizure operations had not amounted to disproportionate interference with the legitimate aim pursued. The Court observed in particular that, after viewing the computer files and emails that had been seized, the investigating judge from the Central Criminal Investigation Court had ordered the deletion of 850 records which he considered to be private, to be covered by professional secrecy or to have no direct bearing on the case. The Court saw no reason to call into question the assessment made by the judge, who had intervened to review the lawfulness of the search and seizure operations and especially to protect legal professional secrecy. Moreover, in response to the applicants' objection that the computer records seized had not been returned to them, the Court noted that the originals had been given back and that there was no obligation to return the copies, which could be retained throughout the limitation period for the crimes in question.

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.

Trabajo Rueda v. Spain

30 May 2017

This case concerned the seizure of the applicant's computer on the grounds that it contained child pornography material. The applicant complained that the police seizure and inspection of his computer had amounted to an interference with his right to respect for his private life and correspondence.

The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention. It first noted that the police access to files in the applicant's personal computer and his conviction had amounted to an interference with his right to respect for his private life. That interference was prescribed by domestic law. It also pursued the legitimate aim of "prevention of crime" and "protection of the rights of others". In this respect, the Court emphasised in particular that "sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims" and that "children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives". However, the Court deemed that the police seizure of the computer and inspection of the files which it contained, without prior judicial authorisation, had not been proportionate to the legitimate aims pursued and had not been "necessary in a democratic society". It found that it was difficult to assess the urgency of the situation requiring the police to seize the files from the applicant's personal computer and to access their content, bypassing the normal requirement of prior judicial authorisation, when in fact the computer in question was already in the hands of the police and prior authorisation could have been obtained fairly quickly without impeding the police inquiries.

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** (right to respect for private life) 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.

Ivashchenko v. Russia

13 February 2018

This case concerned the copying of the data from a photojournalist's laptop by Russian customs officials.

The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention, finding that, overall, the Russian Government had not shown that the legislation and practice applied in the case had provided the necessary safeguards against abuse when it came to applying the customs sampling procedure for electronic data contained in an electronic device.

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** (right to respect for private life) 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.

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** (right to respect for private life) 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.

Buturugă v. Romania

11 February 2020[2]

This case concerned allegations of domestic violence and of violation of the confidentiality of electronic correspondence by the former husband of the applicant, who complained of shortcomings in the system for protecting victims of this type of violence. The applicant complained in particular of the ineffectiveness of the criminal investigation into the domestic violence which she claimed to have suffered. She also complained that her personal safety had not been adequately secured, and criticised the authorities' refusal to consider her complaint concerning her former husband's breach of the confidentiality of her correspondence.

The Court held that there had been a **violation of Article 3** (prohibition of inhuman or degrading treatment) **and Article 8** (right to respect for private life and correspondence) of the Convention on account of the State's failure to fulfil its positive obligations under those provisions. It found in particular that the national authorities had not addressed the criminal investigation as raising the specific issue of domestic violence, and that they had thereby failed to provide an appropriate response to the seriousness of the facts complained of by the applicant. The investigation into the acts of violence had been defective, and no consideration had been given to the merits of the complaint regarding violation of the confidentially of correspondence, which was closely linked to the complaint of violence. On that occasion the Court lastly pointed out that cyberbullying was currently recognised as an aspect of violence against women and girls, and that it could take on a variety of forms, including cyber breaches of privacy, intrusion into the victim's computer and the capture, sharing and manipulation of data and images, including private data.

Gaughran v. the United Kingdom

13 février 2020[3]

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** (right to respect for private life) 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.

Pending applications

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

19 June 2018 (Chamber judgment) – case referred to the Grand Chamber in February 2019

This case concerns a complaint brought by a public interest law firm alleging that legislation permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes breached its privacy rights.

In its Chamber judgment of 19 June 2018, the Court held, unanimously, that there had been no violation of Article 8 (right to respect for private life) of the Convention.

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

[3]. This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention.

The Chamber considered that the relevant legislation amounted to a system of secret surveillance that potentially affected all users of mobile telephones and the Internet, without their being notified. Also, there was no domestic remedy providing detailed grounds in response to a complainant who suspected that his or her communications had been intercepted. On that basis, the Court found it justified to examine the legislation in the abstract. The law firm could claim to be a victim of a violation of the Convention, although it had not brought any domestic proceedings or made a concrete allegation that its communications had actually been intercepted. The mere existence of the legislation amounted in itself to an interference with its rights under Article 8. The Chamber went on to say that, although there were some areas for improvement, overall the Swedish system of bulk interception provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. When coming to that conclusion, the Chamber took into account the State's discretionary powers in protecting national security, especially given the present-day threats of global terrorism and serious cross-border crime. Given those findings, the Chamber considered that there were no separate issues under Article 13 (right to an effective remedy) of the Convention and held that there was no need to examine the foundation's complaint in that respect.
On 4 February 2019 the Grand Chamber Panel accepted the applicant's request that the case be referred to the Grand Chamber.
On 10 July 2019 the Grand Chamber held a hearing in the case.

Big Brother Watch and Others v. the United Kingdom (nos. 58170/13, 62322/14 and 24960/15)

13 September 2018 (Chamber judgment) – case referred to the Grand Chamber in February 2019
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 concerns complaints by journalists, individuals and rights organisations about three different surveillance regimes: (1) the bulk interception of communications; (2) intelligence sharing with foreign governments; and (3) the obtaining of communications data from communications service providers.
In its Chamber judgment of 13 September 2018, the Court held, by five votes to two, that the bulk interception regime violated Article 8 (right to respect for private life) of the Convention as there was insufficient oversight both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, and the safeguards governing the selection of "related communications data" for examination were inadequate. In reaching that conclusion, the Chamber found that the operation of a bulk interception regime did not in and of itself violate the Convention, but noted that such a regime had to respect criteria set down in its case-law. The Chamber also held, by six votes to one, that the regime for obtaining communications data from communications service providers violated Article 8 as it was not in accordance with the law, and that both the bulk interception regime and the regime for obtaining communications data from communications service providers violated Article 10 (freedom of expression) of the Convention as there were insufficient safeguards in respect of confidential journalistic material. It further found that the regime for sharing intelligence with foreign governments did not violate either Article 8 or Article 10. Lastly, the Chamber unanimously rejected complaints made by the third set of applicants under Article 6 (right to a fair trial) of the Convention, about the domestic procedure for challenging secret surveillance measures, and under Article 14 (prohibition of discrimination) of the Convention.
On 4 February 2019 the Grand Chamber Panel accepted the applicants' request that the case be referred to the Grand Chamber.
On 10 July 2019 the Grand Chamber held a hearing in the case.

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

Similar application pending: **Ringler v. Austria (no. 2309/10)**, communicated to the Austrian Government on 6 May 2013.

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 (right to respect for private life and correspondence), 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.

Privacy International and Others v. the United Kingdom (no. 46259/16)

Application communicaed to the UK Government on 19 November 2018
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 – believe that their equipment has been subject to interference known as Computer Network Exploitation or Equipment Interference, colloquially known as "hacking", over an undefined period by the United Kingdom Government Communications Headquarters and/or the Secret Intelligence Service. They complain that the power under section 7 of the Intelligence Services Act[4] is not in accordance with the law, that it contains no requirement for judicial authorisation, that there is no information in the public domain about how it might be used to authorise Equipment Interference, and that there is no requirement for filtering to exclude irrelevant material. They add 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 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 correspondence), 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.

E-mail

Copland v. the United Kingdom

3 April 2007
The applicant was employed by a college of further education, a statutory body administered by the State, as a personal assistant to the principal. From the end of 1995 she was required to work closely with the deputy principal. Her telephone, e-mail and internet usage were subjected to monitoring at the deputy principal's instigation. According to the UK Government, this was in order to ascertain whether the applicant was making excessive use of college facilities for personal purposes.

[4]. 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.

The Court held that there had been a **violation of Article 8** (right to respect for private life and correspondence) of the Convention. It first observed that telephone calls from business premises were *prima facie* covered by the notions of "private life" and "correspondence". It followed logically that e-mails sent from work should be similarly protected, as should information derived from the monitoring of personal internet usage. In the instant case, the Court considered that the collection and storage of personal information relating to the applicant's use of the telephone, e-mail and internet, without her knowledge, had amounted to an interference with her right to respect for her private life and correspondence. While leaving open the question whether the monitoring of an employee's use of a telephone, e-mail or internet at the place of work might be considered "necessary in a democratic society" in certain situations in pursuit of a legitimate aim, the Court concluded that, in the absence of any domestic law regulating monitoring at the material time, the interference was not "in accordance with the law".

Muscio v. Italy

13 November 2007 (decision on the admissibility)

This case concerned the president of a Catholic parents' association who had received unsolicited e-mails (spam) of an obscene nature. Having instituted proceedings against a person or persons unknown, he contested the decision to take no further action on his complaint.

The Court declared **inadmissible**, as being manifestly ill-founded, the applicant's **complaint under Article 8** (right to respect for private and family life) of the Convention. It considered that receiving undesirable messages amounted to interference with the right to respect for private life. However, once connected to the Internet, e-mail users no longer enjoyed effective protection of their privacy and exposed themselves to the risk of receiving undesirable messages. In that context, the legal action brought by the applicant had had no chance of succeeding, since the national authorities and Internet service providers encountered objective difficulties in combating spam. The Court could not therefore require the State to make additional efforts to discharge its positive obligations under Article 8 of the Convention.

Benediktsdóttir v. Iceland

16 June 2009 (decision on the admissibility)

The applicant complained that, by affording her insufficient protection against unlawful publication of her private e-mails in the media, Iceland had failed to secure her rights guaranteed by Article 8 (right to respect for private life and correspondence). She submitted that an unknown third party had obtained the e-mails in question, without her knowledge and consent from a server formerly owned and operated by her former employer who had gone bankrupt. The e-mail communications consisted in particular of direct quotations or paraphrasing of e-mail exchanges between the applicant and the former colleague of a multinational company's Chief Executive Officer and his wishes to find a suitable lawyer to assist him in handing over to the police allegedly incriminating material he had in his possession and to represent him in a future court case against the leaders of the multinational company in question. At the time there was an ongoing public debate in Iceland relating to allegations that undue influence had been exerted by prominent figures on the most extensive criminal investigations ever carried out in the country.

The Court declared the application **inadmissible** as being manifestly ill-founded. It found that there was nothing to indicate that the Icelandic authorities had transgressed their margin of appreciation and had failed to strike a fair balance between the newspaper's freedom of expression and the applicant's right to respect for her private life and correspondence under Article 8 of the Convention.

Helander v. Finland

10 September 2013 (decision on the admissibility)

This case concerned a complaint brought by a prisoner that the prison authority had refused to forward legal correspondence to him, which had been sent to the prison's official e-mail address by his lawyer.

The Court declared the case **inadmissible**, as being manifestly ill-founded, as the applicant's lawyer had immediately been informed that his e-mail would not be conveyed to his client and that lawyer and client remained able at all times to communicate quickly by telephone, letter or personal visit. The Court also recognised that, under Finland's current legislation, lawyer-client confidentiality could not be guaranteed in e-mail correspondence, and that the prison authority therefore had a genuine reason for not forwarding the message on.

Sérvulo & Associados - Sociedade de Advogados, RL v. Portugal

3 September 2015

See above, under "Electronic data".

GPS (Global Positioning System)

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** (right to respect for private life) of the Convention. Given that the criminal investigation had concerned very serious crimes, it found that the GPS surveillance of the applicant had been proportionate.

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** (right to respect for private life) 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.

Internet[5]

Perrin v. the United Kingdom

18 October 2005 (decision on the admissibility)

The case concerned the conviction and sentencing to 30 months' imprisonment of a French national based in the United Kingdom – and operating a United States-based Internet company with sexually explicit content – for publishing obscene articles on Internet.

The Court rejected the applicant's **complaint under Article 10** (freedom of expression) of the Convention as **inadmissible** (manifestly ill-founded). It was satisfied that the criminal conviction was necessary in a democratic society in the interests of the protection of morals and/or the rights of others and that the sentence was not disproportionate.

Paeffgen GmbH v. Germany

18 September 2007 (decision on the admissibility)

The case concerned proceedings brought against the applicant company, engaged in e-commerce, by other companies and private individuals claiming that its registration and use of certain Internet domains breached their trademark rights and / or their rights to a (business) name.

The Court declared **inadmissible**, as being manifestly ill-founded, the applicant company's **complaint under Article 1** (protection of property) **of Protocol No. 1** to the Convention. It found that the court orders requiring the applicant company to cancel the domains had struck a fair balance between the protection of its possessions and the requirements of the general interest (i.e. to prevent the company from continuing to violate third parties' trademark rights).

K.U. v. Finland (application no. 2872/02)

2 December 2008

This case concerned an advertisement of a sexual nature posted about a 12-year old boy on an Internet dating site. Under Finnish legislation in place at the time[6], the police and the courts could not require the Internet provider to identify the person who had posted the ad. In particular, the service provider refused to identify the person responsible, claiming it would constitute a breach of confidentiality.

The Court held that there had been a **violation of Article 8** (right to respect for private and family life) of the Convention. It considered that posting the ad was a criminal act which made a minor a target for paedophiles. The legislature should have provided a framework for reconciling the confidentiality of Internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others, and in particular children and other vulnerable individuals.

Times Newspapers Ltd v. the United Kingdom (nos. 1 & 2)

10 March 2009

The applicant company, owner and publisher of *The Times* newspaper, alleged that the rule under United Kingdom law, whereby a new cause of action in libel proceedings accrues each time defamatory material on the Internet is accessed ("the Internet publication rule"), constituted an unjustifiable and disproportionate restriction on its right to freedom of expression. In December 1999 the applicant newspaper published two

5. See also the factsheet on "Access to Internet and freedom to impart information".
6. A legal framework had been introduced by the time of the European Court of Human Rights' judgment under the Exercise of Freedom of Expression in Mass Media Act.

articles that were allegedly defamatory of a private individual. Both articles were uploaded onto *The Times*' website on the same day as they were published in the paper version of the newspaper. During the subsequent libel proceedings against the applicant newspaper, it was required to add a notice to both articles in the Internet archive announcing that they were subject to libel litigation and were not to be reproduced or relied on without reference to the applicant company's legal department.
In this judgment the Court underlined that, in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. In the present case, it found that there had been **no violation of Article 10** (freedom of expression) of the Convention: since the archives were managed by the newspaper itself and the domestic courts had not suggested that the articles be removed altogether, the requirement to add an appropriate qualification to the Internet version had not been disproportionate.

Willem v. France

16 July 2009
This case concerned the call for a boycott of Israeli products by a mayor, notably via the municipality's internet site. The mayor was subsequently convicted of provoking discrimination.
The Court found that there had been **no violation of Article 10** (freedom of expression) of the Convention. The reasons given by the French courts to justify the interference with the applicant's freedom of expression had been "relevant and sufficient" for the purposes of Article 10. In addition, the fine imposed had been relatively moderate and proportionate to the aim pursued.

Renaud v. France

25 February 2010
The applicant complained of his conviction for defaming and publicly insulting a mayor on the Internet site of the association of which he was president and webmaster.
The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It considered that the applicant's conviction had been disproportionate to the legitimate aim of protecting the reputation and rights of others.

Editorial Board of Pravoye Delo and Shtekel v. Ukraine

5 May 2011
This case mainly concerned the lack of adequate safeguards in Ukrainian law for journalists' use of information obtained from the Internet. In particular, defamation proceedings had been brought against a local newspaper and its editor-in-chief following their publication of a letter downloaded from the Internet alleging that senior local officials were corrupt and involved with the leaders of an organised criminal gang. The domestic courts ruled against the applicants and ordered them to publish an apology and pay 15,000 Ukrainian hryvnias (approximately EUR 2,394), eventually waived via a friendly settlement.
The Court held that the order to the editor-in-chief to apologise had not been done in accordance with the law, and had, therefore, been in **violation of Article 10** (freedom of expression) of the Convention. It further held that there had been a **violation of Article 10** because of the lack of adequate safeguards for journalists using information obtained from the Internet. Notably, "having regard to the role the Internet plays in the context of professional media activities ... and its importance for the exercise of the right to freedom of expression generally ..., the Court consider[ed] that the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press as a 'public watchdog' ..." (§ 64 of the judgment).

Mosley v. the United Kingdom

10 May 2011

This case concerned the publication of articles, images and video footage in the *News of the World* newspaper and on its website which disclosed details of Max Mosley's sexual activities. The applicant complained about the authorities' failure to impose a legal duty on the newspaper to notify him in advance of further publication of the material so that he could seek an interim injunction.

The Court found that there had been **no violation of Article 8** (right to respect for private life) of the Convention. It held in particular that the European Convention on Human Rights did not require media to give prior notice of intended publications to those who feature in them.

Ahmet Yıldırım v. Turkey

18 December 2012

This case concerned a court decision to block access to Google Sites, which hosted an Internet site whose owner was facing criminal proceedings for insulting the memory of Atatürk. As a result of the decision, access to all other sites hosted by the service was blocked. The applicant complained that he was unable to access his own Internet site because of this measure ordered in the context of criminal proceedings without any connection to him or his site. He submitted that the measure infringed his right to freedom to receive and impart information and ideas.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It found that the effects of the measure in question had been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses.

Ashby Donald and Others v. France

10 January 2013

This case concerned the conviction of fashion photographers for copyright infringement following the publication on the Internet site of a fashion company run by two of the applicants, without the authorisation of the fashion houses concerned, of photos taken by the other applicant at fashion shows in 2003.

The Court held that there had been **no violation of Article 10** (freedom of expression) of the Convention. In the circumstances of the case and regard being had to the particularly wide margin of appreciation open to the domestic authorities, the nature and gravity of the penalties imposed on the applicants were not such that the Court could find that the interference in issue was disproportionate to the aim pursued.

Neij and Sunde Kolmisoppi v. Sweden

19 February 2013 (decision on the admissibility)

This case concerned the complaint by two of the co-founders of "The Pirate Bay", one of the world's largest websites for sharing torrent files, that their conviction for complicity to commit crimes in violation of the Copyright Act had breached their freedom of expression.

The Court declared the application **inadmissible** as being manifestly ill-founded. It held that sharing, or allowing others to share, files of this kind on the Internet, even copyright-protected material and for profit-making purposes, was covered by the right to "receive and impart information" under Article 10 (freedom of expression) of the Convention. However, it considered that the domestic courts had rightly balanced the competing interests at stake – i.e. the right of the applicants to receive and impart information and the necessity to protect copyright – when convicting the applicants.

Akdeniz v. Turkey

11 March 2014 (decision on the admissibility)

This case concerned the blocking of access to two websites on the grounds that they streamed music without respecting copyright legislation. The applicant, who had applied to the European Court of Human Rights as a user of the websites in question, complained in particular of a violation of his freedom of expression.

The Court declared the application **inadmissible** (incompatible *ratione personae*), finding that the applicant could not claim to be a "victim" in the sense of Article 34 (right of individual application) of the Convention. While stressing that the rights of internet users are of paramount importance, the Court nevertheless noted that the two music streaming websites had been blocked because they operated in breach of copyright law. As a user of these websites, the applicant had benefited from their services, and he had only been deprived of one way among others of listening to music. The Court further observed that the applicant had at his disposal many means to access to a range of musical works, without thereby contravening the rules governing copyright.

Delfi AS v. Estonia

16 June 2015 (Grand Chamber)

This was the first case in which the Court had been called upon to examine a complaint about liability for user-generated comments on an Internet news portal. The applicant company, which runs a news portal run on a commercial basis, complained that it had been held liable by the national courts for the offensive comments posted by its readers below one of its online news articles about a ferry company. At the request of the lawyers of the owner of the ferry company, the applicant company removed the offensive comments about six weeks after their publication.

The Court held that there had been **no violation of Article 10** (freedom of expression) of the Convention, finding that the Estonian courts' finding of liability against the applicant company had been a justified and proportionate restriction on the portal's freedom of expression, in particular, because: the comments in question had been extreme and had been posted in reaction to an article published by the applicant on its professionally managed news portal run on a commercial basis; the steps taken by the applicant to remove the offensive comments without delay after their publication had been insufficient; and the 320 euro fine had by no means been excessive for the applicant, one of the largest Internet portals in Estonia.

Cengiz and Others v. Turkey

1 December 2015

This case concerned the blocking of access to *YouTube*, a website enabling users to send, view and share videos. The applicants complained in particular of an infringement of their right to freedom to receive and impart information and ideas.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention, finding in particular that the applicants, all academics in different universities, had been prevented from accessing *YouTube* for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas. The Court also observed that *YouTube* was a single platform which enabled information of specific interest, particularly on political and social matters, to be broadcast and citizen journalism to emerge. The Court further found that there was no provision in the law allowing the domestic courts to impose a blanket blocking order on access to the Internet, and in the present case to *YouTube*, on account of one of its contents.

Kalda v. Estonia

19 January 2016

This case concerned a prisoner's complaint about the authorities' refusal to grant him access to three Internet websites, containing legal information, run by the State and by the Council of Europe. The applicant complained in particular that the ban under Estonian law on his accessing these specific websites had breached his right to receive information via the Internet and prevented him from carrying out legal research for court proceedings in which he was engaged.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It found in particular that Contracting States are not obliged to grant prisoners access to Internet. However, if a State is willing to allow prisoners access, as is

the case in Estonia, it has to give reasons for refusing access to specific sites. In the specific circumstances of the applicant's case, the reasons, namely the security and costs implications, for not allowing him access to the Internet sites in question had not been sufficient to justify the interference with his right to receive information. Notably, the authorities had already made security arrangements for prisoners' use of Internet via computers specially adapted for that purpose and under the supervision of the prison authorities and had borne the related costs. Indeed, the domestic courts had undertaken no detailed analysis as to the possible security risks of access to the three additional websites in question, bearing in mind that they were run by an international organisation and by the State itself.

See also: **Jankovskis v. Lithuania**, judgment of 17 January 2017.

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary

2 February 2016

This case concerned the liability of a self-regulatory body of Internet content providers and an Internet news portal for vulgar and offensive online comments posted on their websites following the publication of an opinion criticising the misleading business practices of two real estate websites. The applicants complained about the Hungarian courts' rulings against them, which had effectively obliged them to moderate the contents of comments made by readers on their websites, arguing that that had gone against the essence of free expression on the Internet.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It reiterated in particular that, although not publishers of comments in the traditional sense, Internet news portals had to, in principle, assume duties and responsibilities. However, the Court considered that the Hungarian courts, when deciding on the notion of liability in the applicants' case, had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation. Notably, the Hungarian authorities accepted at face value that the comments had been unlawful as being injurious to the reputation of the real estate websites.

Dallas v. the United Kingdom

11 February 2016

This case concerned the applicant's conviction for contempt of court as a result of her conducting Internet research in relation to the criminal case she was trying as a juror. The applicant complained that the common law offence of contempt of court had not been sufficiently clear.

The Court held that there had been **no violation of Article 7** (no punishment without law) of the Convention. It found found in particular that the test for contempt of court applied in her case had been both accessible and foreseeable. The law-making function of the courts had remained within reasonable limits and the judgment in her case could be considered, at most, a step in the gradual clarification of the rules of criminal liability for contempt of court through judicial interpretation. Any development of the law had been consistent with the essence of the offence and could be reasonably foreseen.

Pihl v. Sweden

7 February 2017 (decision on the admissibility)

The applicant had been the subject of a defamatory online comment, which had been published anonymously on a blog. He made a civil claim against the small non-profit association which ran the blog, claiming that it should be held liable for the third-party comment. The claim was rejected by the Swedish courts and the Chancellor of Justice. The applicant complained to the Court that by failing to hold the association liable, the authorities had failed to protect his reputation and had violated his right to respect for his private life.

The Court declared the application **inadmissible** as being manifestly ill-founded. It noted in particular that, in cases such as this, a balance must be struck between an individual's right to respect for his private life, and the right to freedom of expression

enjoyed by an individual or group running an internet portal. In light of the circumstances of this case, the Court found that national authorities had struck a fair balance when refusing to hold the association liable for the anonymous comment. In particular, this was because: although the comment had been offensive, it had not amounted to hate speech or an incitement to violence; it had been posted on a small blog run by a non-profit association; it had been taken down the day after the applicant had made a complaint; and it had only been on the blog for around nine days.

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** (right to respect for private life and correspondence) 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.

M.L. and W.W. c. Allemagne (nos. 60798/10 and 65599/10)

28 June 2018

This case concerned the refusal by the Federal Court of Justice to issue an injunction prohibiting three different media from continuing to allow Internet users access to documentation concerning the applicants' conviction for the murder of a famous actor and mentioning their names in full. The applicants complained of an infringement of their right to respect for their private life

The Court held that there had been **no violation of Article 8** (right to respect for private life) of the Convention. It shared in particular the findings of the German Federal Court, which had reiterated that the media had the task of participating in the creation of democratic opinion, by making available to the public old news items that had been preserved in their archives. The Court also reiterated that the approach to covering a given subject was a matter of journalistic freedom and that Article 10 (freedom of expression) of the Convention left it to journalists to decide what details ought to be published, provided that these decisions corresponded to the profession's ethical norms. The inclusion in a report of individualised information, such as the full name of the person in question, was an important aspect of the press's work, especially when reporting on criminal proceedings which had attracted considerable attention that remained undiminished with the passage of time. Lastly, the Court noted that during their most recent request to reopen proceedings in 2004, the applicants had themselves contacted the press, transmitting a number of documents while inviting journalists to keep the public informed. This attitude put a different perspective on their hope of obtaining anonymity in the reports, or on the right to be forgotten online. In conclusion, having regard to the margin of appreciation left to the national authorities when weighing up divergent interests, the importance of maintaining the accessibility of press reports which had been recognised as lawful, and the applicants' conduct vis-à-vis the

press, the Court considered that there were no substantial grounds for it to substitute its view for that of the Federal Court of Justice.

Magyar Jeti Zrt v. Hungary

4 December 2018

This case concerned the applicant company being found liable for posting a hyperlink to an interview on YouTube which was later found to contain defamatory content. The applicant company complained that by finding it liable for posting the hyperlink on its website the domestic courts had unduly restricted its rights.

The Court held that there had been a **violation of Article 10** (freedom of expression) of the Convention. It underscored in particular the importance of hyperlinking for the smooth operation of the Internet and distinguished the use of hyperlinks from traditional publishing – hyperlinks directed people to available material rather than provided content. Updating its case-law on these issues, the Court set down elements which need to be considered under Article 10 when looking at whether posting a hyperlink could lead to liability and said that an individual assessment was necessary in each case. In the present case, the Court found that the Hungarian domestic law on objective (strict) liability for disseminating defamatory material had excluded the possibility of any meaningful assessment of the applicant company's right to freedom of expression in a situation where the courts should have scrutinised the issue carefully. Such objective liability for using a hyperlink could undermine the flow of information on the Internet, dissuading article authors and publishers from using such links if they could not control the information they led to. That could have a chilling effect on freedom of expression on the Internet. The Court therefore found that, overall, the applicant company had suffered an undue restriction of its rights.

Høiness v. Norway

19 March 2019

This case concerned the Norwegian courts' refusal to impose civil liability on an Internet forum host after vulgar comments about the applicant had been posted on the forum. The applicant complained that the authorities had violated her rights by not sufficiently protecting her right to protection of her reputation and by requiring her to pay litigation costs to the extent seen in her case.

The Court held that there had been **no violation of Article 8** (right to respect for private life) of the Convention, findind that the Norwegian courts had sufficiently safeguarded the applicant's rights under that provision. It considered in particular that the national courts had acted within their discretion ("margin of appreciation") when seeking to establish a balance between the applicant's rights under Article 8 and the opposing right to freedom of expression under Article 10 of the Convention of the news portal and host of the debate forums. Moreover, the domestic courts' rulings on litigation costs being awarded to the defendants had not as such violated Article 8 of the Convention.

Pending applications

Kharitonov v. Russia (no. 10795/14)

Application communicated to the Russian Government on 27 April 2017

The applicant alleges in particular that the blocking of a third party's website located on the same IP address as his own had the disproportionate effect of blocking access to his website.

The Court gave notice of the application to the Russian Government and put questions to the parties under Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention.

Hurbain v. Belgium (no. 57292/16)

Application communicated to the Belgian Government on 7 September 2018

This application concerns a civil court order that the applicant, responsible for publishing the newspaper *Le Soir*, had to provide anonymity in its online archive to a driver who

had been responsible for a 1994 road accident, based on the right to be forgotten. The applicant alleges that the interference in question, based on Article 1382 of the Civil Code, was unclear and not foreseeable.
The Court gave notice of the application to the Belgian Government and put questions to the parties under Article 10 (freedom of expression) of the Convention.

Mobile telephone applications

Magyar Kétfarkú Kutya Párt v. Hungary

20 January 2020

This case concerned a political party's mobile application which allowed voters to photograph, anonymously upload and comment on invalid votes cast during a referendum on immigration in 2016. The applicant party complained about a violation of its rights under Article 10 (right to freedom of expression) of the Convention.
The Grand Chamber found in particular that the provision of domestic election law relied on by the authorities (a breach of the principle of the exercise of rights in accordance with their purpose) had not allowed the applicant party to foresee that it could be penalised for providing such an app, which had been an exercise of its freedom of expression. It concluded that the considerable uncertainty about the potential effects of the provision had exceeded what was acceptable under the Convention and that the lack of sufficient precision in the law to rule out arbitrariness and allow the applicant party to regulate its conduct had led to a **violation of Article 10** (freedom of expression) of the Convention.

Musical copyright

SIA AKKA/LAA v. Latvia

12 July 2016

This case concerned a complaint about the restriction on the copyright of authors' musical work. The applicant, an organisation responsible for managing the copyright of the musical works of a large number of Latvian and international authors, complained about decisions by the national courts ordering the applicant organisation and two radio companies to enter into a licence agreement and to set an equitable royalty rate. The applicant organisation notably alleged that those decisions had restricted the exclusive rights of the authors they represented to freely conclude licence agreements for the use of their musical works.
The Court held that there had been **no violation of Article 1** (protection of property) **of Protocol No. 1** to the Convention and **no violation of Article 6 § 1** (right to fair trial) of the Convention. It found in particular that the Latvian authorities had struck a fair balance between the demands of the public interest (namely, the radio companies' interest in obtaining a licence allowing them to legally broadcast work as well as the general public's interest in having access to musical works), on the one hand, and the rights of the applicant organisation to obtain equitable remuneration from the use of musical work, on the other. Indeed, the effort to maintain a balance between the competing interests could be seen in their decisions, which had observed that protected works were being broadcast without a valid licence over an extended period of time and that that situation had to a certain extent been due to the applicant organisation's limited efficiency in carrying out negotiations with the radio companies.

Radio communications

Brambilla and Others v. Italy

23 June 2016

This case concerned the conviction of three journalists who intercepted radio communications between *carabinieri* in order to arrive quickly at crime scenes and report on them for their local newspaper.

The Court held that there had been **no violation of Article 10** (freedom of expression) of the Convention. Stressing the notion of responsible journalism and noting that the decisions of the domestic courts had been duly reasoned and had focused primarily on the need to protect national security and prevent crime and disorder, the Court found in particular that the Italian courts had made an appropriate distinction between on the one hand the duty of the three journalists to comply with domestic law, which prohibited in general terms the interception by any persons of communications not addressed to them, including those of the law-enforcement agencies, and on the other hand the pursuit of their journalistic activities, which had not been restricted per se. The Court also noted that the penalties ordered by the domestic courts, consisting in the seizure of the radio equipment and the imposition of custodial sentences, had not been disproportionate, as the sentences of the three journalists had been suspended and the authorities had not prohibited them from bringing news items to the public's attention.

Satellite dish

Khurshid Mustafa and Tarzibachi v. Sweden

16 December 2008

This case concerned a court decision not to prolong a private tenancy agreement owing to the refusal by the tenants, a married couple of Iraqi origin with three minor children, to remove a satellite dish used to receive television programmes from their country of origin. The landlord offered to allow the applicants to stay if they agreed to remove the satellite dish, but they refused and had to move out. The applicants complained of a violation of their freedom to receive information.

The Court held that there had been a **violation of Article 10** (freedom of expression – freedom to receive information) of the Convention. It observed in particular that the satellite dish had enabled the applicants and their children to receive television programmes in Arabic and Farsi from their native country and region. That information – which included political and social news and, almost equally importantly, cultural expression and entertainment – was of particular interest to them as an immigrant family who wished to maintain contact with the culture and language of their country of origin. It had not been claimed that the applicants had any other means of receiving such programmes at the time or that they could have placed the satellite dish elsewhere. Nor could news obtained from foreign newspapers and radio programmes in any way be equated with information available via television broadcasts. The landlord's concerns about safety had been examined by the domestic courts, who had found that the installation did not pose any real safety threat. Moreover, the fact that the applicants had effectively been evicted from their home with their three children had been disproportionate to the aim pursued.

Telecommunications

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** (right to respect for private life and correspondence) 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.

Breyer v. Germany

30 January 2020[7]

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** (right to respect for private life) 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.

Use of hidden cameras

Haldimann and Others v. Switzerland

24 February 2015

This case concerned the conviction of four journalists for having recorded and broadcast an interview of a private insurance broker using a hidden camera, as part of a television documentary intended to denounce the misleading advice provided by insurance brokers. The applicants complained that their sentence to payment of fines had amounted to a disproportionate interference in their right to freedom of expression.
In this case, the Court was for the first time called on to examine an application concerning the use of hidden cameras by journalists to provide public information on a subject of general interest, whereby the person filmed was targeted not in any personal capacity but as a representative of a particular professional category. The Court held

[7]. This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention.

that, in the applicants' case, there had been a **violation of Article 10** (freedom of expression) of the Convention, considering in particular that the interference in the private life of the broker, who had turned down an opportunity to express his views on the interview in question, had not been serious enough to override the public interest in information on malpractice in the field of insurance brokerage. The Court further also asserted that the applicants deserved the benefit of the doubt in relation to their desire to observe the ethics of journalism as defined by Swiss law, citing the example of their limited use of the hidden camera.

Bremner v. Turkey

13 October 2015

This case concerned the broadcasting of a television documentary in which the applicant, who was shown promoting his evangelical Christian beliefs, was described as a "foreign pedlar of religion" engaged in covert activities in Turkey. The applicant alleged that the broadcasting of the documentary and the refusal of the judicial authorities to grant his request for compensation had breached his right to respect for his private life.
The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention, finding in particular that the broadcasting of the applicant's image without blurring it could not be regarded as a contribution to any debate of general interest for society, regardless of the degree of public interest in the question of religious proselytising. As regards the method used, the Court was of the view that a technique as intrusive and as damaging to private life must in principle be used restrictively. The Court was not unaware that, in certain cases, the use of hidden cameras might prove necessary for journalists when information was difficult to obtain by any other means. However, that tool had to be used in compliance with ethical principles and with restraint.

See also:

Erdtmann v. Germany

5 January 2016 (decision on the admissibility)

Video surveillance

Peck v. the United Kingdom

28 January 2003

In this case the applicant, who was suffering from depression, complained about the disclosure in the media of footage from a closed-circuit television (CCTV) camera mounted in the street showing him walking alone with a kitchen knife in his hand (he had subsequently attempted suicide by cutting his wrists, but the CCTV footage did not show this), which had resulted in images of himself being published and broadcast widely. He further complained of the lack of an effective domestic remedy in that regard.
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** (right to respect for private life) of the Convention. Furthermore, at the relevant time, the applicant had not had an effective remedy for breach of confidence, **in violation of Article 13** (right to an effective remedy) **read in conjunction with Article 8** of the Convention.

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** (right to respect for private life) 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.

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 (right to respect for private life) 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. It 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.

Riina v. Italy

11 March 2014 (decision on the admissibility)

The applicant, who was sentenced to life imprisonment for having committed very serious crimes, including mafia-type conspiracy and multiple assassinations, complained of the fact that he was under constant video surveillance in his cell, including in the toilets. He contended that the domestic remedies available in respect of these measures were ineffective.

The Court declared the application **inadmissible** under Articles 3 (prohibition of inhuman or degrading treatment) and 8 (right to respect for private and family life) of the Convention, finding that the applicant had not exhausted the domestic remedies available to him to appeal against the application of the video surveillance measure.

Vasilică Mocanu v. Romania

6 December 2016

This case concerned the conditions in which the applicant was held on police premises. The applicant also alleged that his cell had been fitted with a system of permanent CCTV monitoring by which he was filmed.

The Court held that there had been a **violation of Article 8** (right to respect of private life) of the Convention, finding that the surveillance of the applicant by a video camera which was present in the cell where he had been placed on the premises of the County police had not been in accordance with the domestic law.

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** (right to respect for private life) 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.

Gorlov and Others v. Russia

2 July 2019

This case concerned the permanent video surveillance of detainees in their cells by closed-circuit television cameras. The applicants complained, in particular, that constant surveillance of their cells, at times by female guards, had violated their right to respect for their private life.

The Court held that there had been a **violation of Article 8** (right to respect for private life) of the Convention, finding that the measure in question had not been in accordance with the law. Although the Court could accept that it might be necessary to monitor certain areas of penal institutions, or certain detainees on a permanent basis, it found in particular that the existing legal framework in Russia could not be regarded as being sufficiently clear, precise and detailed to afford appropriate protection against arbitrary interference by the public authorities with the right to respect for private life. The Court also held that there had been a **violation of Article 13** (right to an effective remedy) of the Convention **in conjunction with Article 8** in respect of two of the applicants, finding that they had not had at their disposal an effective domestic remedy for their complaint of a violation of the right to respect for their private life.

See also: **Izmestyev v. Russia**, judgment of 27 August 2019.

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** (right to respect for private life) 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.

Media Contact:
Tel.: +33 (0)3 90 21 42 08