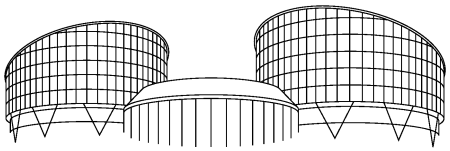

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Guide to the Case-Law of the of the European Court of Human Rights

Data protection

Updated on 28 February 2023

Prepared by the Registry. It does not bind the Court.

Publishers or organisations wishing to translate and/or reproduce all or part of this Guide in the form of a printed or electronic publication are invited to complete the contact form: *request to reproduce or republish a translation* for information on the authorisation procedure.

If you wish to know which translations of the Case-Law Guides are currently under way, please see the list of *pending translations*.

This Guide was originally drafted in French. It is updated regularly and, most recently, on 28 February 2023. It may be subject to editorial revision.

The Case-Law Guides are available for downloading at *https://ks.echr.coe.int*. For publication updates please follow the Court's Twitter account at *https://twitter.com/ECHR_CEDH*.

© Council of Europe/European Court of Human Rights, 2023

Table of contents

Table of contents 3

Note to readers 6

Introduction 7

I. Basic definitions and principles of data protection 7

A. Data protection terminology 7
1. Concept of personal data and its scope 7
2. Specific categories of data 11
a. So-called "sensitive" categories 11
i. Data revealing racial or ethnic origin 11
ii. Data revealing political opinions, and religious or other beliefs, including philosophical 11
iii. Data revealing trade union membership 12
iv. Genetic and biometric data 12
v. Data concerning health, sex life or sexual orientation 14
vi. Data on criminal offences and convictions 15
b. Other categories of data 15
i. Employment data 15
ii. Financial data 16
iii. Traffic data 16
iv. Voice samples 18
v. GPS location data 18
vi. Photography 19

B. The two aspects (negative and positive) of data protection 21

C. The three data protection "tests" 24
1. Whether the interference was lawful 24
2. Whether the interference pursued a legitimate aim 27
3. Whether the interference was "necessary in a democratic society" 28
a. Requirement to minimise the amount of data collected or recorded 29
b. Requirement of accuracy and updating of data 29
c. Requirement that data be retained for no longer than is necessary to fulfil the purpose for which they were recorded 30
d. Requirement to limit the use of data to the purpose for which they were recorded 31
e. Requirement of transparency of data processing procedures 31

II. Data protection and the right to respect for private life (Article 8 of the Convention) 32

A. Data operations liable to infringe the right to respect for private life 32
1. Personal data collection 32
a. Data collection by the authorities via covert surveillance 32
i. Telephone tapping and metering 33
ii. Interception of pager messages 34
iii. Audio-surveillance and video-surveillance 34
iv. Geolocation of vehicle by GPS 35
v. Surveillance by private detectives 35

vi. Monitoring of correspondence 36
vii. Covert surveillance, espionage and mass surveillance operations 36
b. Data collection by employers in the workplace 37
c. Data collection for use in evidence in court cases 40
i. Searches and seizures 40
ii. Compulsory medical acts for the purposes of cellular sampling 43
d. Personal data collection in a medical context 44
e. Compulsory communication of personal data 45
2. Retention of personal data 46
a. Storage of personal data for the purposes of combating crime 46
i. Indiscriminate and undifferentiated nature of data stored 47
ii. Data retention period 48
iii. Safeguards concerning the destruction or deletion of data stored 50
iv. Guarantees aimed at regulating access by third parties and protecting data integrity and confidentiality 52
b. Retention of medical data 53
c. Online storage of personal data for journalistic purposes 53
3. Disclosure of personal data 53
a. Impact of prior consent 54
b. Disclosure of data in the context of judicial proceedings 56
c. Disclosure of data for the protection of public health 58
d. Disclosure of data for the protection of national security 59
e. Disclosure of data for the protection of the economic well-being of the country 59
f. Mass disclosure of personal data 60
B. Data subjects' rights 60
1. Right of access to one's own data 60
2. Right of rectification 63
3. Right to data deletion ("right to be forgotten") 64
4. Right to benefit from special procedural safeguards and an effective procedural framework to uphold one's rights 67

III. Interaction with other provisions of the Convention and its Protocols .. 70

A. Data protection and substantive rights 71
1. Data protection and freedom of thought, conscience and religion (Article 9 of the Convention) 72
2. Data protection and freedom of expression (Article 10 of the Convention) 73
3. Data protection and prohibition of discrimination (Article 14 of the Convention) 76
4. Data protection and right to peaceful enjoyment of possessions (Article 1 of Protocol No. 1) 77
5. Data protection and freedom of movement (Article 2 of Protocol No. 4) 77
B. Data protection and procedural rights 79
1. Right to a fair trial (Article 6 of the Convention) 79
a. General guarantees (Article 6 § 1 of the Convention) 79
i. Equality of arms and respect for the adversarial principle in proceedings involving sensitive or confidential information 80
ii. Reasoning of judicial decisions and data protection 80
iii. Use in evidence of personal data collected unlawfully or in breach of Article 8 .. 81
iv. Public hearing and public pronouncement of judgment and confidentiality of data 81
v. Length of judicial proceedings concerning data protection 82
b. Specific guarantees (Article 6 §§ 2 and 3 of the Convention) 82

i. Data protection and the right to be presumed innocent (Article 6 § 2 of the Convention)..... 82
ii. Data protection and defence rights (Article 6 § 3 (b) of the Convention)..... 83
2. Right to an effective remedy (Article 13 of the Convention)..... 84
3. Right to liberty and security (Article 5 of the Convention)..... 86

IV. Modern-day challenges of data protection..... 87

A. Technological advances, algorithms and artificial intelligence..... 87
B. Internet and search engines..... 88
C. Data transfers and data flows..... 90

List of cited cases..... 91

Note to readers

This Guide is part of the series of Case-Law Guides published by the European Court of Human Rights (hereafter "the Court", "the European Court" or "the Strasbourg Court") to inform legal practitioners about the fundamental judgments and decisions delivered by the Court. This particular Guide analyses and sums up the case-law under different Articles of the European Convention on Human Rights (hereafter "the Convention" or "the European Convention") relating to data protection. It should be read in conjunction with the case-law guides by Article, to which it refers systematically.

The case-law cited has been selected among the leading, major, and/or recent judgments and decisions.*

The Court's judgments and decisions serve not only to decide those cases brought before the Court but, more generally, to elucidate, safeguard and develop the rules instituted by the Convention, thereby contributing to the observance by the States of the engagements undertaken by them as Contracting Parties (*Ireland v. the United Kingdom*, 18 January 1978, § 154, Series A no. 25, and, more recently, *Jeronovičs v. Latvia* [GC], no. 44898/10, § 109, 5 July 2016).

The mission of the system set up by the Convention is thus to determine, in the general interest, issues of public policy, thereby raising the standards of protection of human rights and extending human rights jurisprudence throughout the community of the Convention States (*Konstantin Markin v. Russia* [GC], 30078/06, § 89, ECHR 2012). Indeed, the Court has emphasised the Convention's role as a "constitutional instrument of European public order" in the field of human rights (*Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, § 156, ECHR 2005-VI, and, more recently, *N.D. and N.T. v. Spain* [GC], nos. 8675/15 and 8697/15, § 110, 13 February 2020).

Protocol No. 15 to the Convention recently inserted the principle of subsidiarity into the Preamble to the Convention. This principle "imposes a shared responsibility between the States Parties and the Court" as regards human rights protection, and the national authorities and courts must interpret and apply domestic law in a manner that gives full effect to the rights and freedoms defined in the Convention and the Protocols thereto (*Grzęda v. Poland* [GC], § 324).

*. The case-law cited may be in either or both of the official languages (English or French) of the Court and the European Commission of Human Rights. Unless otherwise indicated, all references are to a judgment on the merits delivered by a Chamber of the Court. The abbreviation "(dec.)" indicates that the citation is of a decision of the Court and "[GC]" that the case was heard by the Grand Chamber. Chamber judgments that were not final when this update was published are marked with an asterisk (*).

Introduction

1. Technological progress has led to a quantum leap in surveillance, interception of communications and data retention, in turn leading to major challenges for personal data protection. Since the *Leander v. Sweden* judgment of 1987, in which the "old" Court analysed, for the first time, the question of the storage by a public authority of an individual's personal data, the case-law of the Convention organs in this field has seen significant development.

2. Over the years the Court has examined many situations in which questions related to this issue have been raised. A broad spectrum of operations involving personal data, such as the collection, storage, use and dissemination of such data, is now covered by a body of case-law of the Convention organs which will be described in this guide. This case-law has developed in line with the rapid evolution in information and communication technologies.

I. Basic definitions and principles of data protection

3. The right to the protection of personal data is not an autonomous right among the various Convention rights and freedoms. The Court has nevertheless acknowledged that 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, home and correspondence, as guaranteed by Article 8 of the Convention (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 137; *Z v. Finland,* 1997, § 95). This Article is the main vector through which personal data is protected in the Convention system, even though considerations related to this protection may also come into play under other provisions of the Convention and its Protocols.

A. Data protection terminology

4. The development of technologies has led to an increase in the types of operations involving personal data that can constitute "automatic processing". In spite of the Court's generous approach to the definition of the notion of "private life", which has enabled it to build a body of case-law in line with the evolution of society, a given data processing operation will not necessarily fall within the scope of Article 8 or necessarily undermine one of the interests protected by this Article.

1. Concept of personal data and its scope

5. In its judgments the Court explains the concept of "personal data" with reference to Council of Europe Convention no. 108 for the protection of individuals with regard to automatic processing of personal data of 28 January 1981, which entered into force in 1985 and was updated in 2018 ("Convention 108"), whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1) (*Amann v. Switzerland* [GC], 2000, § 65; *Haralambie v. Romania*, 2009, § 77). The Court has clearly indicated that, under Article 2 of Convention 108, the concept of personal data is defined as "any information relating to an identified or identifiable individual" (*Amann v. Switzerland* [GC], 2000, § 65; *Haralambie v. Romania,* 2009, § 77).

6. Such data cover not only information directly identifying an individual (the "data subject"), such as surname and forename (*Guillot v. France*, 1996, §§ 21-22; *Mentzen v. Latvia* (dec.), 2004; *Güzel Erdagöz v. Turkey*, 2008, § 43; *Garnaga v. Ukraine*, 2013, § 36; *Henry Kismoun v. France,* 2013, § 25; *Hájovský v. Slovakia*, 2021 §§ 11-12 and 41), but also any element indirectly identifying a person such as a dynamic IP (Internet Protocol) address (*Benedik v. Slovenia*, 2018, §§ 107-108).

7. Even though the question of personal data protection seems mainly to concern individuals, as regards their Article 8 right to respect for their private life, legal entities are also entitled to rely on this right before the Court if they are directly affected by a measure which breaches their right to respect for their "correspondence" or "home". This was the case, for example, where a company had been ordered to provide a copy of all data on a server shared with other companies (*Bernh Larsen Holding AS and Others v. Norway*, 2013, § 106) or where the Ministry of Defence, under a warrant, had intercepted the communications of civil liberties NGOs (*Liberty and Others v. the United Kingdom*, 2008, §§ 56-57). However, in a case concerning measures involving the protection of personal data of members of a religious organisation and respect for their "private life", the organisation was not directly affected, and was thus not a "victim" within the meaning of Article 34 of the Convention (*Avilkina and Others v. Russia*, 2013, § 59).

8. Personal data can take very different forms. For example:

- Internet subscriber information associated with specific dynamic IP addresses assigned at certain times (*Benedik v. Slovenia*, 2018, §§ 108-109).
- Recordings taken for use as voice samples, being of a permanent nature and subject to a process of analysis directly relevant to identifying a person in the context of other personal data (*P.G. and J.H. v. the United Kingdom*, 2001, § 59).
- Cellular samples and DNA profiles (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 70-77) or finger prints (ibid., § 84) which, notwithstanding their objective and irrefutable character, contained unique information on the individual concerned and allowed his/her precise identification in a wide range of circumstances (ibid., § 85).
- Information on a given individual obtained from banking documents, whether involving sensitive details or professional activity (*M.N. and Others v. San Marino*, 2015, §§ 51 et seq.).
- Data on the occupation of an identified or identifiable individual collected and stored by the police (*Khelili v. Switzerland*, 2011, § 56).
- Data on Internet and messaging (Yahoo) usage by an employee in the workplace, obtained through surveillance (*Bărbulescu v. Romania* [GC], 2017, §§ 18, 74-81).
- A copy of electronic data seized in a law firm, even though it had not been deciphered, transcribed or officially attributed to their owners (*Kırdök and Others v. Turkey*, 2019, § 36).
- Data collected in the context of non-covert video surveillance in a university (*Antović and Mirković v. Montenegro*, 2017, §§ 44-45).
- Information on the taxable income and assets of a large number of individuals, notwithstanding the fact that the public could access such data under certain conditions (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 138).
- Data on the birth and abandonment of an individual, including information needed to discover the truth about an important aspect of personal identity (*Gaskin v. the United Kingdom*, 1989, § 39; *Mikulić v. Croatia*, 2002, §§ 54-64; *Odièvre v. France* [GC], 2003, §§ 28-29).
- Data included in a divorce settlement, comprising details as to the division of matrimonial assets, the custody and residence of minor children, the alimony agreement and an overview of the assets/income of the applicant (*Liebscher v. Austria*, 2021, §§ 31 and 68).

9. Under Article 2 of Convention 108, "data processing" includes: "any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data". The development of technologies has led to an increase in the types of operations involving personal data that can constitute processing; the Court has identified the following typical examples:

- The collection by the police from an Internet provider of subscriber information associated with an individual's specific dynamic IP address (*Benedik v. Slovenia*, 2018, §§ 108-109).
- The fact of gathering and storing public information on an individual, for example about his/her political activity (*Rotaru v. Romania* [GC], 2000, §§ 43-44; *Association "21 December 1989" and Others v. Romania*, 2011, §§ 167-168; *Amann v. Switzerland* [GC], 2000, §§ 65-67; *Catt v. the United Kingdom*, 2019, § 93).
- The listing of an individual in a national judicial database of sex offenders (*Gardel v. France*, 2009, § 58), and the collection and storage of a suspect's fingerprints (*M.K. v. France*, 2013, § 29).
- The covert recording in a police station, for permanent storage, of voice samples to be used in identifying the individuals concerned, by a process of analysis in the context of other personal data (*P.G. and J.H. v. the United Kingdom*, 2001, §§ 59-60).
- The filming of an individual in a police interview room by cameras installed for security reasons and totally visible, with the permanent recording of the footage and its inclusion in a montage for further use (*Perry v. the United Kingdom*, 2003, § 41).
- The systematic collection and retention of GPS monitoring data indicating the whereabouts and public movements of the subject (*Uzun v. Germany*, 2010, §§ 49-53).
- The publication in a magazine of an article illustrated by photos of celebrities taken without their knowledge (*Von Hannover v. Germany (no. 2)* [GC], 2012, §§ 95-99).
- The recording and disclosure to media of CCTV footage showing an individual trying to commit suicide in a public place (*Peck v. the United Kingdom*, 2003, §§ 59-63).
- The recording and storage by police of data on an individual's supposed occupation (*Khelili v. Switzerland*, 2011, § 56).
- The disclosure by a psychiatric hospital to journalists of highly sensitive confidential information about the private life of a patient (*Mockutė v. Lithuania*, 2018, § 99).
- The collection by the State, as part of anti-doping measures in sport, of information on the whereabouts and daily pursuits, even at weekends, of high-level athletes (*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, 2018, §§ 155-159).
- The systematic scanning and uploading of prisoners' private correspondence, both incoming and outgoing, onto the National Judicial Network Server (*Nuh Uzun and Others v. Turkey*, 2022, §§ 80-82).

10. Such measures are almost always regarded by the Court as interferences, with varying degrees of seriousness, with the right to respect for private life, home or correspondence of the data subjects.

11. However, not all personal data operations fall within the scope of Article 8 or automatically interfere with the corresponding rights. Thus in the case of *Mehmedovic v. Switzerland* (dec.), 2018 (§ 18), the Court took the view that sparse information concerning the applicant, which had been gathered coincidentally and was of no relevance for the investigation in question, had in no way constituted systematic or permanent gathering of data and thus did not interfere with her right to respect for her private life. Moreover, in the case of *Cakicisoy and Others v. Cyprus* (dec.), 2014 (§§ 50-52), the fact that the authorities had taken blood samples from the applicants to extract their DNA profile for an exhumation programme to identify the remains of their deceased relatives, and that the samples were destroyed when the consent forms expired, was not considered to be an interference with the applicants' right to respect for their private life.

12. It can be seen from the Court's case-law that personal data operations fall within the scope of Article 8 if information has been collected on a precise individual (*Amann v. Switzerland* [GC], 2000, §§ 66-67; *Rotaru v. Romania* [GC], 2000, §§ 43-44), if the data in question have been the subject of systematic or permanent recording (*Uzun v. Germany*, 2010, § 51), if they have been used in an

analysis process directly intended to identify an individual in the light of other personal data (*P.G. and J.H. v. the United Kingdom*, 2001, § 57) or if they have been made public in a manner or to an extent which exceeds what the subjects could reasonably have expected (*Peck v. the United Kingdom,* 2003, §§ 58-59; *Perry v. the United Kingdom,* 2003, § 38). Other considerations will be the specific context in which information on an individual 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* [GC], 2008, § 67).

13. A significant element, although not necessarily decisive, is whether an individual is reasonably entitled to expect protection of his/her private life (*Perry v. the United Kingdom,* 2003, § 37; *Bărbulescu v. Romania* [GC], 2017, § 80). As to on-line activities, the anonymity of personal information will be a key factor in that assessment and the fact that a subscriber to an Internet service provider had not hidden his/her dynamic IP address was not decisive in the assessment of whether his expectation of privacy was reasonable from an objective standpoint (*Benedik v. Slovenia*, 2018, § 116). In the workplace, an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary (*Bărbulescu v. Romania* [GC], 2017, §§ 80-81). Video recordings made in a public place using surveillance mechanisms may fall within Article 8 where their disclosure, by its manner or extent, goes beyond what the individuals could reasonably have expected (*Peck v. the United Kingdom*, 2003, § 62; *Perry v. the United Kingdom,* 2003, §§ 41-43). As regards press articles about the arrest of a television actor, illustrated by photos, the Court found that the actor's "legitimate expectation" of having his private life effectively protected was reduced by the fact that he had "actively sought the limelight" by revealing details of his private life in a number of interviews (*Axel Springer AG v. Germany* [GC], 2012, § 101).

14. Concerning the nature of the data collected, some types of personal data and certain processing methods are more problematic than others because they disclose more sensitive information on the conduct, opinions or feelings of individuals (*Uzun v. Germany*, 2010, § 52, where the Court compared data collected by GPS with data collected by video or audio surveillance devices). The storage or disclosure, without the subject's consent, of highly intimate or sensitive data, concerning for example an individual's health, necessarily fall within the scope of Article 8 (*Z v. Finland,* 1997, § 71; *Radu v. Republic of Moldova*, 2014, § 27; *Mockutė v. Lithuania*, 2018, §§ 93-95). Given the nature and the amount of personal information contained in cellular samples, their retention *per se* must be regarded as interfering with the right to respect for the private lives of the individuals concerned, even if only a limited part of this information is actually extracted or used by the authorities and no immediate detriment is caused (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 70-77).

15. The fact that personal data are already in the public domain or can be accessed by the public does not necessarily remove such data from the protection of Article 8 (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 134). Data of a public nature may fall within the "private life" of an individual when they are collected and stored in a systematic manner (*P.G. and J.H. v. the United Kingdom*, 2001, § 57; *Peck v. the United Kingdom,* 2003, §§ 58-59; *Perry v. the United Kingdom,* 2003, § 38), even without using secret surveillance methods (*Rotaru v. Romania* [GC], 2000, §§ 43-44; *Antović and Mirković v. Montenegro*, 2017, §§ 44-45). Article 8 of the Convention provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that Article 8 rights may be engaged (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 137).

16. In most cases where the processing of personal data was intended to allow the authorities to conduct an investigation into the data subject or to collect evidence in judicial proceedings before the domestic courts, the Court has found that such processing fell within the scope of Article 8 and had entailed interference with the respect for the private life of the person concerned (*Perry v. the United Kingdom,* 2003, §§ 39-43; *Uzun v. Germany,* 2010, §§ 51-52; *Vukota-Bojić v. Switzerland*, 2016, §§ 57-

59 ; *López Ribalda and Others v. Spain* [GC], 2019, § 94 ; contrast *Lupker and Others v. the Netherlands*, 1992, on the use by the police, for the purpose of identifying the applicants, of photographs which had been voluntarily handed to the authorities or which had been taken by the police in connection with previous arrests; *Friedl v. Austria*, 1994, §§ 50-51, on the taking of photographs by the authorities during a demonstration with a view to opening an investigation against the applicants for traffic offences).

17. Lastly, for Article 8 to come into play, the results of the personal data processing must attain a certain level of seriousness and in a manner causing prejudice to personal enjoyment of the right to respect for private life (*M.L. and W.W. v. Germany*, 2018, § 88). In the case of *Vučina v. Croatia* (dec.) 2019 (§ 50), the Court rejected as incompatible *ratione materiae* a complaint about the publication of a photograph in a women's magazine under an erroneous title which had referred to the applicant as someone else. In the Court's view, the low degree of seriousness of that error and the very limit inconvenience caused was not sufficient for Article 8 to be engaged.

2. Specific categories of data

18. Certain highly intimate or sensitive information clearly justifies reinforced protection, in the Court's view. Other categories of data must also be given attention, in view of technological developments which are broadening the possibilities of access to such data and resulting in greater interoperability.

a. So-called "sensitive" categories

19. Under Article 6 of Convention 108, personal data revealing racial origin, political opinions, religious or other beliefs, and information on an individual's health or sex life, or on any criminal convictions, cannot be automatically processed unless domestic law provides for appropriate safeguards. Information falling within these categories, described by the Court as "sensitive", warrant a heightened degree of protection in its view.

i. Data revealing racial or ethnic origin

20. An individual's ethnic identity must be regarded as an important element of private life (*S. and Marper v. the United Kingdom*, [GC], 2008, § 66; *Ciubotaru v. Moldova*, 2010, § 49). Data is of particular concern where they might reveal a person's ethnic or other origin, bearing in mind the rapid pace of developments in the field of genetics and information technology (*S. and Marper v. the United Kingdom* [GC], 2008, § 71). Samples and DNA profiles contain much sensitive information and allow the authorities to establish genetic relationships between individuals and assess their likely ethnic origin (ibid., §§ 72-77; *Aycaguer v. France,* 2017, § 33). In a case concerning the recording of an individual's ethnic origin on the official registers, the Court, emphasising the highly sensitive nature of the recording of such data, acknowledged the existence of a positive obligation on the part of the State to put in place a procedure to enable the data subject to have his/her recorded ethnicity changed on the basis of objectively verifiable evidence (*Ciubotaru v. Moldova*, 2010, §§ 52-59).

ii. Data revealing political opinions, and religious or other beliefs, including philosophical

21. Data revealing political opinions are regarded as a "sensitive" category of personal data and, in the Court's view, it is unacceptable for the national authorities to disregard this aspect by processing such data in accordance with ordinary domestic rules, without taking account of the need for eightened protection (*Catt v. the United Kingdom*, 2019, § 112). In the 2019 case of *Catt v. the United Kingdom*, concerning the storage in a police database of data relating to a peaceful demonstrator, the national courts had merely made reference to the general data protection law in examining the lawfulness of the interference. The Court found a violation of Article 8, pointing out that the sensitive nature of the data in question should have constituted a key element of the case before the domestic

courts, as it was before the Court (ibid., § 112). The Court likewise found a violation of Article 8 in *M.D. and Others v. Spain*, 2022, (§§ 63-64) concerning a report drawn up by the police in respect of judges and magistrates, who exercised their functions in Catalonia and who had signed a manifesto in which they had set out their legal opinion in favour of the possibility of the Catalan people's exercising the so-called "right to decide", the report revealing, in particular, the political views of some of the applicants.

22. The right to the protection of personal data revealing the religious or other beliefs, including philosophical, of an individual was examined by the Court in the cases of *Sinan Işık v. Turkey*, 2010 (§ 37) and *Mockutė v. Lithuania*, 2018 (§ 117). As to the indication of religion on the applicants' identity cards, the Court emphasised the importance of the right to protection of data relating to religious beliefs, which constituted one of the most vital elements making up the identity of believers and their conception of life, as protected by Article 9 of the Convention (*Sinan Işık v. Turkey*, 2010, § 37).

iii. Data revealing trade union membership

23. Personal data revealing the trade union membership of an individual may also be "sensitive" and thus warrant heightened protection. In the case of *Catt v. the United Kingdom*, 2019 (§ 112), information had been collected by the police about the applicant's participation in demonstrations organised by a number of trade unions, in particular his name, presence, date of birth and address. In certain cases his appearance had also been described, together with photos taken during the demonstrations in question (ibid., § 10). Engaging in peaceful protest has specific protection under Article 11 of the Convention, which also contains special protection for trade unions (ibid., § 123). While the collection by the police of personal data about the applicant could be regarded as justified, there was no pressing need, in the Court's view to retain the applicant's data, in the absence of any rules setting a definitive maximum time limit on the retention of such data (ibid., §§ 117-119).

iv. Genetic and biometric data

24. The Court has dealt with a number of cases concerning the collection or retention of:

- cellular samples (*Van der Velden v. the Netherlands* (dec.), 2005; *Schmidt v. Germany* (dec.), 2006; *S. and Marper v. the United Kingdom* [GC], 2008; *Canonne v. France* (dec.), 2015; *Caruana v. Malta* (dec.), 2018; *Trajkovski and Chipovski v. North Macedonia*, 2020; *Boljević v. Serbia*, 2020);
- DNA profiles (*Van der Velden v. the Netherlands* (dec.), 2005; *Schmidt v. Germany* (dec.), 2006; *S. and Marper v. the United Kingdom* [GC], 2008; *W. v. the Netherlands* (dec.), 2009; *Peruzzo and Martens v. Germany* (dec.), 2013; *Canonne v. France* (dec.), 2015; *Aycaguer v. France*, 2017; *Mifsud v. Malta*, 2019; *Gaughran v. the United Kingdom*, 2020; *Trajkovski and Chipovski v. North Macedonia*, 2020; *Dragan Petrović v. Serbia*, 2020);
- fingerprints (*McVeigh, O'Neill and Evans v. the United Kingdom*, 1981; *Kinnunen v. Finland*, 1993; *S. and Marper v. the United Kingdom* [GC], 2008; *Dimitrov-Kazakov v. Bulgaria*, 2011; *M.K. v. France*, 2013; *Suprunenko v. Russia* (dec), 2018; *Gaughran v. the United Kingdom*, 2020; *P.N. v. Germany*, 2020); *Willems v. the Netherlands* (dec.), 2021);
- palm prints (*P.N. v. Germany*, 2020);
- voice samples (*P.G. and J.H. v. the United Kingdom*, 2001; *Allan v. the United Kingdom*, 2002; *Doerga v. the Netherlands*, 2004; *Vetter v. France*, 2005; *Wisse v. France*, 2005).

25. Bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today (*S. and Marper v. the United Kingdom* [GC], 2008, § 71).

26. As regards cellular samples, given the nature and amount of personal information they contain, their retention *per se* must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (ibid., § 73; *Amann v. Switzerland* [GC], 2000, § 69).

27. On the subject of DNA profiles, the possibility of drawing inferences from them as to an individual's ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life, calling for heightened protection (*S. and Marper v. the United Kingdom* [GC], 2008, § 76). While the information contained in the profiles may be considered objective and irrefutable, their capacity to provide a means of identifying genetic relationships between individuals is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned, notwithstanding any safeguards or the degree of probability of detriment in a given case (ibid., § 75; *Amann v. Switzerland* [GC], 2000, § 69). This conclusion is not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 74-75).

28. Concerning fingerprints, as they objectively contain unique information about the individual concerned, allowing his or her identification with precision in a wide range of circumstances, the retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant (ibid., § 84). Even though the retention of fingerprints on the authorities' records, in connection with an identified or identifiable individual, may have a lesser impact on private life than the retention of cellular samples and DNA profiles (ibid., § 69), it may give rise to important private-life concerns, notwithstanding the objective and irrefutable character of such data (ibid., § 85, departing from the case-law based on the Commission decision in *Kinnunen v. Finland,* 1996). In the case of *Willems v. the Netherlands* (dec.), 2021, complaints concerning the obligation under the Passport Act to have fingerprints taken when applying for a passport, as well as the storage of such prints on an electronic chip, following the incorporation into domestic law (with no latitude left to national authorities) of the EU Regulation on standards for security features and biometrics in passports and travel documents issued by Member States, were dismissed as manifestly ill-founded owing to the "presumption of equivalent protection" in EU law (ibid., §§ 26-36).

29. Because of the information they contain, the retention of cellular samples and DNA profiles has a greater impact on private life than the retention of fingerprints (*S. and Marper v. the United Kingdom* [GC], 2008, § 86). However, while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in determining the question of justification, the retention of fingerprints constitutes an interference *per se* with the right to respect for private life.

30. In certain circumstances, especially in paternity proceedings, the authorities may compel an individual to undergo a DNA test, provided the individual's defence rights are respected and the domestic courts strike a fair balance between the interests at stake (*Mifsud v. Malta*, 2019, §§ 77-78). Article 8 does not as such prohibit recourse to a medical procedure in defiance of the will of a suspect or a witness, in order to obtain evidence, as such methods, including in the civil sphere, are not in themselves contrary to the rule of law and natural justice (ibid., § 71). A system which has no means of compelling a putative father to comply with a court order for DNA tests to be carried out can in principle be considered to be compatible with the obligations deriving from Article 8, especially if it provides alternative means enabling an independent authority to determine the paternity claim speedily (*Mikulić v. Croatia*, 2002, §§ 55, 64).

v. Data concerning health, sex life or sexual orientation

31. Information concerning an individual's health constitutes a key element of private life (*Yvonne Chave née Jullien v. France,* 1991, § 75; *L.L. v. France*, 2006; *Radu v. Moldova*, 2014; *L.H. v. Latvia*, 2014, § 56; *Konovalova v. Russia*, 2014, §§ 27, 41; *Y.Y. v. Russia*, 2016, § 38; *Surikov v. Ukraine*, 2017; *Frâncu v. Romania*, 2020, § 52). Respect for the confidentiality of this information 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. These considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection. (*Z v. Finland*, 1997, § 96; *Kiyutin v. Russia*, 2011, § 64; *Armonienė v. Lithuania*, 2008, § 40; *Biriuk v. Lithuania*, 2008, § 39; *I. v. Finland*, 2008, § 38; *C.C. v. Spain*, 2009, § 33; *Y. v. Turkey* (dec.), 2015, § 65; *P.T. v. Republic of Moldova*, 2020, §§ 5-6, 26; *Y.G. v. Russia*, 2022, § 45). The disclosure of such data may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism (*Z v. Finland*, 1997, § 96; *C.C. v. Spain*, 2009, § 33; *P. and S. v. Poland*, 2012, § 128; *Avilkina and Others v. Russia,* 2013, § 45; *Y. v. Turkey* (dec.), 2015, § 65; *Y.G. v. Russia*, 2022, § 45).

32. The interest in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued. Such interference cannot be compatible with Article 8 of the Convention unless it is justified by an overriding requirement in the public interest (*Z v. Finland*, 1997, § 96). In view of the highly intimate and sensitive nature of information concerning a person's HIV status, any State measures compelling communication or disclosure of such information without the consent of the patient call for the most careful scrutiny on the part of the Court (ibid., § 96).

33. The Court thus found a violation of Article 8 for example in the cases of *Z v. Finland*, 1997 (§§ 113-114), on account of the publication of the identity and HIV status of a woman in a judgment, delivered during criminal proceedings against her husband, which was reported on by the press; *L.L. v. France*, 2006 (§§ 32-48), for the reproduction in a divorce decree of an extract from a personal medical document; *I. v. Finland*, 2008 (§§ 35-49), for insufficient protection against unauthorised access to the medical file of an HIV-positive nurse; *C.C. v. Spain*, 2009 (§§ 26-41), for the publication of the applicant's identity in a judgment related to his HIV status; *P. and S. v. Poland*, 2012 (§§ 128-137), for the disclosure of information by a public hospital by a pregnant girl who wished to have an abortion after being raped; *Konovalova v. Russia*, 2014 (§§ 39-50), where the applicant had complained about having to give birth in front of medical students without her consent; *P.T. v. Republic of Moldova*, 2020 (§§ 24-33), for the unnecessary presence of sensitive medical data on a certificate intended for various uses; *Frâncu v. Romania*, 2020 (§ 52), for a refusal to grant a private hearing, in a corruption case against a mayor, on an application for release on health grounds; and *Y.G. v. Russia*, 2022 (§§ 46-53), where the applicant complained that a database containing, in particular, his health data had been available for sale at a market.

34. Information on an individual's mental health constitutes highly sensitive data (*Mockutė v. Lithuania,* 2018, § 94, on the disclosure of data on a patient's mental health by a psychiatric hospital; *Malanicheva v. Russia* (dec.), 2016, §§ 13, 15-18, concerning the recording in a hospital file of data on the applicants' compulsory placement), like data revealing sexual identification or orientation (*Dudgeon v. the United Kingdom*, 1981, § 41, *J.L. v. Italy*, 2021, § 136, and *Drelon v. France*, 2022, § 79) and an individual's sex life, such as data on an abortion transmitted from one public authority to another without the data subject's consent (*M.S. v. Sweden*, 1997, §§ 41-42). Domestic legislation must afford appropriate guarantees to prevent any communication or disclosure of such data which is not compliant with the safeguards under Article 8 (*Z v. Finland*, 1997, § 95).

vi. Data on criminal offences and convictions

35. Data concerning offences, criminal proceedings, convictions or related preventive measures constitute a category of data which warrant heightened protection under Article 6 of Convention 108 (*M.M. v. the United Kingdom*, 2012, § 188). Any processing of personal data concerning an individual against whom charges have been dropped (*Brunet v. France,* 2014, §§ 38-40), who has been cautioned (*M.M. v. the United Kingdom*, 2012, §§ 188-190), convicted and sentenced (*Gardel v. France*, 2009, § 58 ; *Peruzzo and Martens v. Germany* (dec.), 2013, § 44; *Trajkovski and Chipovski v. North Macedonia*, 2020, § 46) or subjected to a related preventive measure such as being detained in a police station (*Suprunenko v. Russia*, (dec.), 2018, § 61), will constitute an interference with the data subject's right to respect for his or her private life.

36. In the Court's view, although data contained in a criminal record are, in one sense, public information, their systematic storing in central records means that they are available for disclosure long after the event when everyone other than the person concerned is likely to have forgotten about it. Thus as the conviction or caution itself recedes into the past, it becomes a part of the person's private life which must be respected (*M.M. v. the United Kingdom*, 2012, § 188), all the more so where the data concern an individual's distant past (*B.B. v. France*, 2009, § 57; *Catt v. the United Kingdom*, 2019, § 93; *M.L. and W.W. v. Germany*, 2018, §§ 98-100).

37. A measure involving the retention, in the police registers, of an individual's identification data, fingerprints and identity photos may have serious consequences for him or her, making daily life more difficult (*Dimitrov-Kazakov v. Bulgaria*, 2011, §§ 8, 10, 13, 30). In a case concerning the listing of an individual as an "offender" in police records, after he was questioned about a rape, and the retention of this entry even though no charges were brought, the Court found a violation of Article 8 on finding that the data subject, precisely on account of the entry in question, had been subject to several police checks in connection with rape complaints or disappearances of young girls (ibid., §§ 8, 10, 13, 30).

b. Other categories of data

38. In addition to the data described as "sensitive", other categories of personal data are also of concern, especially with the increasingly sophisticated surveillance techniques and the capacity of information and communication technologies to make the daily life of data subjects more difficult.

i. Employment data

39. The recording of employment-related data about an identified or identifiable individual and their storage constitute an interference with the data subject's right to respect for his private and family life under Article 8 (*Khelili v. Switzerland*, 2011, § 56; *Sõro v. Estonia*, 2015, §§ 49 and 56; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, §§ 95-96). Given that information collected by the authorities and retained in their records are nowadays the subject of automatic processing which considerably facilitates access to such data and their transmission, such measures could have serious consequences capable of harming the reputation of individuals or of making their daily life more difficult. The Court found a violation of Article 8 in *Khelili v. Switzerland*, 2011 (§ 64), where the applicant had been recorded as a "prostitute" by the police, an entry subsequently corrected and replaced by "seamstress" in the database, and *Sõro v. Estonia*, 2015 (§ 63), where the applicant was obliged to quit his job after the disclosure of data about his employment as a driver for the former security services. In *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 (§§ 95-96), where the applicant's employer had installed a GPS system in the applicant's company vehicle with the aim of monitoring the distances travelled in the course of his professional activity and, as applicable, on private journeys, the Court considered that the collected information constituted personal data. It further emphasised that the employees had not been authorised to deactivate the GPS system, so it

remained active around the clock, seven days a week, with the result that the surveillance was permanent and systematic which clearly interfered with the applicant's private life[1].

ii. Financial data

40. Information retrieved from an individual's banking documents constitutes personal data, whether it is sensitive private information on information on the data subject's professional dealings (*M.N. and Others v. San Marino,* 2015, § 51; *G.S.B. v. Switzerland*, 2015, § 51). The copying of banking data and the subsequent storage by the authorities of such data, acts which fall under the notion of both "private life" and "correspondence", amount to interference for the purposes of Article 8 (*M.N. and Others v. San Marino*, 2015, § 55).

41. The Court has examined the issue of the collection, processing and disclosure of financial data in the context of: a criminal investigation (*M.N. and Others v. San Marino*, 2015, §§ 7-9, 53-55); the widespread publication by the press of financial data for the purpose of a debate on a matter of general interest (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, §§ 172-173); the obligation for a lawyer to reveal data covered by professional privilege in declaring suspicions about unlawful activities on the part of clients such as money laundering (*Michaud v. France,* 2012, §§ 91-92); the transmission of financial data to the authorities of another State which is not a party to the Convention (*G.S.B. v. Switzerland*, 2015, § 50); and lastly, the rejection of a claim concerning the disclosure of information on the applicant's tax identification number and tax return during a television report about a criminal case against her husband (*Samoylova v. Russia*, 2021, §§ 83 and 90-93).

42. The existence of a public interest in providing access to, and allowing the collection of, large amounts of tax data does not necessarily or automatically mean that there is also a public interest in disseminating *en masse* such raw data in unaltered form without any analytical input (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, §§ 172-178, 198).

43. Even though, in tax matters, the State's margin of appreciation is broader when it comes to the protection of purely financial data which do not include any data that is personal or closely linked to the identity of the data subject (*G.S.B. v. Switzerland*, 2015, § 93), private life considerations come into play in situations where tax data have been compiled on a precise individual, or where they have been made public in a manner or to a degree that goes beyond what the data subject could reasonably have foreseen (*M.N. and Others v. San Marino*, 2015, §§ 52-53 ; *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 136).

iii. Traffic data

44. Traffic data include data obtained from telephone operators which identify the person to or from which a communication is transmitted, together with the date, time and length of the communication, but not relating to the content of that communication (*Malone v. the United Kingdom,* 1984, §§ 83-84; *Copland v. the United Kingdom*, 2007, § 43). In the context of a criminal investigation, the process known as "metering", involving the use of a device (a meter check printer) which registers the numbers dialled on a particular telephone and the time and duration of each call, without monitoring or intercepting the communications, constitutes an interference with the private life of the data subject (*Malone v. the United Kingdom*, 1984, §§ 83-84). The use of such data and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone" (*Malone v. the United Kingdom*, 1984, § 84; *Copland v. the United Kingdom*, 2007, § 43). In the Court's view, release of that information to the

[1] See also "GPS location data" below.

police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (*Malone v. the United Kingdom*, 1984, § 84).

45. The practice of "metering", which will not breach Article 8 when carried out, for example, by the supplier of a telephone service to ensure that the subscriber is correctly charged, is to be distinguished by its very nature from interception of calls (*Malone v. the United Kingdom*, 1984, §§ 83-84; *P.G. and J.H. v. the United Kingdom*, 2001, § 42). A court order sent to a telephone company to obtain data on calls made to and from an individual's different mobile phones, and requiring it to collect cell site data for the subsequent tracking of his movements, was not necessarily incompatible with Article 8 in so far as it was authorised by law and ensured sufficient safeguards against arbitrariness (*Ben Faiza v. France*, 2018, §§ 56, 59, 69). The Court found no violation of Article 8 in a case where such orders had to be authorised beforehand by a public prosecutor on pain of nullity and could be challenged before the courts, and where the data obtained could be excluded from evidence in the event of illegality (ibid., §§ 79, 73).

46. The personal data of users of prepaid SIM cards, such as the names, addresses and telephone numbers of mobile telephone subscribers, collected by the service providers, cannot be regarded as "insignificant" (*Breyer v. Germany*, 2020, §§ 92-95). The mere storage, by communication service providers, of such subscriber data, constitutes an interference with the data subject's private life, regardless of any subsequent use (ibid., § 92). Such interference is of a rather limited nature (ibid., § 95) and national authorities enjoy a certain margin of appreciation in this area, in the absence of any European consensus (ibid., § 90). A lack of notification about a retrieval procedure will not be incompatible with Article 8 in so far as there is supervision by an independent authority which is competent to examine, where deemed justified, whether it is acceptable to transmit data to a requesting authority, and a possibility of appeal by anyone who believes that his or her rights have been infringed through a retrieval procedure or a data request (ibid., §§ 103-107).

47. As regards Internet connection data, it may allow the identification of the user, for example his or her IP address and e-mail address, the addressee(s) of the communication, information on the communication material used and any additional services requested or used and their supplier (*Benedik v. Slovenia*, 2018, § 96). In the Court's view, the subscriber information associated with specific dynamic IP addresses assigned at certain times constitutes personal data. It is not publicly available and therefore cannot be compared to the information found in the traditional telephone directory or a public database of vehicle registration numbers (ibid., § 108).

48. The acquisition of related communications data in the context of bulk interception is not necessarily less intrusive than acquisition of the content of the communications (*Centrum för rättvisa v. Sweden* [GC], 2021, 277, and *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 363). The interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content. That being said, in view of the different character of related communications data and the different ways in which they are used by the intelligence services, as long as the aforementioned safeguards are in place, the legal provisions governing their treatment may not necessarily have to be identical in every respect to those governing the treatment of content (*Centrum för rättvisa v. Sweden* [GC], 2021, § 278; and *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 364).

49. An overriding requirement of confidentiality of connection data may, in some circumstances, prove incompatible with Article 8 if it impedes an effective criminal investigation with the aim of identifying and prosecuting the perpetrator of an offence committed via the Internet (*K.U. v. Finland,* 2008, § 49). The guarantee of telecommunications and Internet subscribers to respect for their private life must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others (ibid., § 49).

iv. Voice samples

50. "Bugging" operations are aimed at intercepting an individual's conversations through the installation of listening devices on private property (*Vetter v. France*, 2005, §§ 10, 20) or in public places (*P.G. and J.H. v. the United Kingdom*, 2001, §§ 38, 63 ; *Allan v. the United Kingdom*, 2002, § 35 ; *Doerga v. the Netherlands*, 2004, § 43 ; *Wisse v. France*, 2005, § 29).

51. The covert taping of a person's voice and the keeping of a permanent record which is subject to a process of analysis directly relevant to identifying that person, in the context of other personal data, constitute personal data processing which interferes with the data subject's right to respect for his or her private life (*P.G. and J.H. v. the United Kingdom*, 2001, §§ 59-60). In a case where there was no domestic law regulating the use of covert listening devices installed by the police on their own premises or on private premises, the Court found a violation of Article 8 (ibid., §§ 38, 63).

52. The bugging of conversations using listening devices, like the interception of telephone calls, represents a serious interference with the data subject's right to respect for his or her private life (*Vetter v. France*, 2005, § 26). It must therefore be based on a particularly precise "law": in this field too, the existence of clear and detailed rules appears indispensable, especially as the relevant technical processes are continually being perfected (ibid., § 26). In the Court's view, the "law" must provide citizens with "appropriate safeguards" against the same sort of abuse as could be feared in the case of telephone tapping (ibid., § 26). Thus, in particular, the categories of individuals that may be subjected to such a measure and the type of offences that could justify it will have to be defined; the court will have to set a time-limit on the implementation of such a measure; it will also be necessary to lay down the conditions for drawing up reports of the intercepted conversations, the precautions to be taken to communicate the recordings in an intact and complete state, for possible review by a judge and by the defence, and the circumstances in which the tapes must be deleted or destroyed, especially after a discontinuance decision or acquittal (ibid., § 26, referring to the criteria on intercept evidence as set out in *Kruslin v. France*, 1990, § 35).

53. Where an individual's voice has been recorded without the minimum degree of protection required by the rule of law in a democratic society, it will constitute a violation of Article 8 (*Wisse v. France,* 2005, § 34 on the recording and subsequent use of conversations in a prison visiting room; *Allan v. the United Kingdom*, 2002, § 36, on the installation of a listening device in a prison cell).

v. GPS location data

54. Data collected by a GPS device constitute personal data in so far as they may indicate the whereabouts of an individual and his or her public movements (*Uzun v. Germany*, 2010, §§ 51-52; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, § 95). The processing and use of such data can be regarded as an interference with the data subject's right to respect for private life (http://hudoc.echr.coe.int/eng?i=001-100344*Uzun v. Germany*, 2010, §§ 51-52; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, § 96). GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. (http://hudoc.echr.coe.int/eng?i=001-100344*Uzun v. Germany*, 2010, § 52).

55. As this type of measure must be considered to interfere less with the private life of the data subject than the interception of his or her telephone conversations, the relatively strict standards laid down and applied in the specific context of telephone tapping are not applicable as such to the surveillance via GPS of an individual's movements (ibid., § 66). In order to examine whether, in a given case, an individual who is subjected to a GPS geolocation measure has been afforded adequate protection against arbitrary interference with the exercise of his Article 8 rights, the Court will apply more general principles in examining the foreseeability of the law (ibid., § 66 and references cited in

§ 63). The issuance of a warrant by an independent body is not always necessary and subsequent judicial review of GPS surveillance will provide sufficient protection against arbitrariness (ibid., § 72).

56. The installation of a real-time geolocation device on an individual's vehicle in the context of a criminal investigation into drug trafficking was found by the Court to breach Article 8 in a case where domestic law (neither statute law nor case-law) did not at the relevant time indicate with sufficient clarity as to how, and to what extent, the authorities were entitled to use their discretionary power in this area (*Ben Faiza v. France*, 2018, §§ 58-61).

57. However, in another case where the Court examined the question of an individual's personal data collected through geolocation and the use of the data in criminal proceedings against him, it found no violation of Article 8 (*Uzun v. Germany*, 2010, §§ 60-74). Judicial review and the possibility of excluding evidence obtained from illegal GPS surveillance constituted an important safeguard, as it discouraged the investigating authorities from collecting evidence by unlawful means (ibid., § 72). The circumstances that domestic law subjected the authorisation of the impugned surveillance measure to very stringent conditions, that the GPS surveillance had only been ordered after other less intrusive means of investigation had proved ineffective, and that it had been carried out for a relatively short period of time, were also taken into account in examining the proportionality of the interference (ibid., §§ 77-81).

58. In *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 (§§ 95-96 and 105-125) the applicant's employer had installed a GPS system in the applicant's company vehicle with the aim of monitoring the distances travelled in the course of his professional activity and, as applicable, on private journeys. The Court observed that the said system made it possible to monitor the movements of the vehicle in real time: it was thus possible to locate geographically the persons or persons who were supposed to use it at a given moment or continuously. In the Court's view, such information constituted personal data. It further emphasised that the employees had not been authorised to deactivate the GPS system, so it remained active around the clock, seven days a week, with the result that the surveillance was permanent and systematic which clearly interfered with the applicant's private life. At the same time, the Court considered that the domestic courts had carefully balanced the competing interests at stake namely, the applicant's right to respect for his private life and his employer's right to ensure the smooth running of the company, taking into account the legitimate aim pursued by the company, namely the right to monitor its expenditure. The Court therefore found no violation of Article 8 of the Convention.

vi. Photography

59. The right to the protection of one's image is one of the essential components of personal development and presupposes the right to control the use of that image (*Reklos and Davourlis v. Greece*, 2009, §§ 40-43). Except where an individual has knowingly or accidentally laid himself open to the possibility of having his photograph taken in the context of an activity that was likely to be recorded or reported in a public manner, the effective protection of one's image presupposes, in principle, obtaining the consent of the person concerned at the time the picture is taken and not simply if and when it is published (ibid., §§ 37, 40). However, this principle is not absolute. The status of public or newsworthy figure may, in certain circumstances, on public-interest grounds, justify the recording of a person's image without his or her knowledge and its dissemination without his or her consent[2].

60. In the case of individuals arrested or charged, the objective usefulness of photos taken by the authorities after arresting an individual suspected of committing an offence may render their

[2] See also Guide to Article 10 of the Convention (freedom of expression) on the publication of photos for journalistic purposes.

retention "necessary in a democratic society" for the purposes of countering crime (*Suprunenko v. Russia* (dec.), 2018, §§ 63-65). The mere fact that a photo is taken of a suspect and is included in a database does not necessarily entail a stigma of suspicion or guilt (ibid., § 64). In the case of *Murray v. the United Kingdom* [GC], 1994 (§§ 92-93), the taking and retention, without his consent, of a photograph of a person suspected of a terrorism offence had not been disproportionate to the aim pursued of preventing terrorism, a legitimate aim in a democratic society. It could not be regarded as falling outside the legitimate bounds of the process of investigation of terrorist crime for the competent authorities to record and retain basic personal details concerning the arrested person or even other persons present at the time and place of arrest (ibid., § 93). The Court also declared manifestly ill-founded an application concerning the retention in the Interior Ministry's computer system of the applicant's photo, which had been taken by the authorities when he was arrested by the police on suspicion of committing an offence (*Suprunenko v. Russia* (dec.), 2018, § 65). In the Court's view, even though the information thus collected and stored on the police computer was personal in nature, it could not be deemed intimate or sensitive (ibid., § 64).

61. The Court, however, found a violation of Article 8 where the police had given the press photographs of individuals who had been arrested or charged without their prior consent (*Sciacca v. Italy*, 2005, §§ 29-31; *Khoujine and Others v. Russia*, 2008, §§ 115-118), or where they had invited television crews to illegally film an applicant in the police station and to broadcast the footage (*Toma v. Romania*, 2009, §§ 90-93; *Khmel v. Russia*, 2013, § 41), or in a case where the displaying of an applicant's photo on a notice-board of wanted persons had not been in accordance with the law (*Guiorgui Nikolaïchvili v. Georgia*, 2009, §§ 129-131).

62. In the Court's view, the retention for an unlimited duration of the photograph of an individual suspected of committing an offence who had not been found guilty carried a higher risk of stigmatisation than the retention of data on individuals who had been convicted of an offence (*S. and Marper v. the United Kingdom* [GC], 2008, § 122; *Gaughran v. the United Kingdom*, 2020, §§ 82-84). The duration of the retention period is not necessarily decisive in assessing whether a State has overstepped the acceptable margin of appreciation in establishing the relevant regime for the retention of personal data, but rather the existence and functioning of certain safeguards (ibid., § 88).

63. The facial recognition and facial mapping techniques that may nowadays be applied to photographs are increasingly complex and the domestic courts must take account of this in examining the necessity of any interference with the right to respect for private life of an individual whose photograph has been taken by the authorities (ibid., §§ 67-70).

64. In the case of *Gaughran v. the United Kingdom*, 2020 (§§ 97-98), where the authorities had decided on the indefinite retention of the photograph of an individual convicted of driving with excess alcohol, in addition to his DNA profile and fingerprints, the Court found a violation of Article 8. In deciding on that retention of personal data, without reference to the seriousness of the offence and in the absence of any real possibility of review, the authorities had failed to strike a fair balance between the competing public and private interests. Even though the State was afforded a slightly wider margin of appreciation in respect of the retention of photographs compared to that of DNA profiles (ibid., §§ 84, 96), that widened margin was not sufficient for the retention of such data to be proportionate in all circumstances, in particular where there were no relevant safeguards or any real possibility of review (ibid., § 96).

65. In the case of *P.N. v. Germany*, 2020 (§§ 76-91) the Court found no violation of Article 8 as regards a collection ordered by the police, following the opening of fresh criminal proceedings against an individual who had been previously convicted, of information identifying him, such as photographs of his face and body, especially any tattoos, together with fingerprints and palmprints. In view of the relatively limited intrusiveness and duration of the collection of the identification data in question, the limited impact of the data retention on the applicant's daily life, the deletion of the data after five years, and the fact that the data was stored in a police database subject to safeguards and

individualised review, the impugned measure had constituted a proportionate interference with the applicant's right to respect for his private life.

66. In a different context, the Court found in the case of *Reklos and Davourlis v. Greece*, 2009 (§§ 41-43), that there had been a violation of Article 8 on the ground that the taking of photographs of a newborn baby in a clinic and their retention by the photographer in a form permitting identification, with the possibility of subsequent use, had taken place against the parents' will. Similarly a violation was found in the cases of *Hájovský v. Slovakia*, 2021 (§§ 46-49), as regards the publication in the press of non-blurred images of the applicant, taken covertly under pretences, and *Volodina v. Russia (no. 2)*, 2021, § 68, which concerned the authorities' failure to protect a women against repeated cyberviolence by her husband, who had created fake profiles in her name and had published her intimate photos.

67. In the case of *Vučina v. Croatia* (dec.), 2019 (§§ 34-51), the mere fact that a name that was not that of the applicant, without having any negative connotation, had been indicated by mistake in the caption to a photograph in a women's magazine could not be regarded as a particularly substantial interference with the data subject's right to respect for her private life.

68. In the case of *Von Hannover v. Germany (no. 2)* [GC], 2012 (§§ 114-126), the refusal by the domestic courts to ban the publication of a photograph of a famous couple taken without their knowledge had not constituted a violation of Article 8, given that the national courts had carefully weighed in the balance the publishing company's right to freedom of expression on the one hand, and the applicants' right to respect for their private life on the other. In doing so they had attached fundamental importance to the question whether the photos, considered in the light of the accompanying articles, had contributed to a debate of general interest. They had also examined the circumstances in which the photos had been taken.

69. In the case of *Kahn v. Germany*, 2016 (§§ 63-76) the Court found no violation of Article 8 where a publisher had not been ordered to pay any sum for having breached a ban on the publication of photos of two children of a former goalkeeper of the German national football team. The Court clarified that it was not possible to deduce from Article 8 of the Convention a principle whereby, in order to protect a person's private life in an effective manner, an order requiring a publisher to pay a sum for failing to comply with an injunction not to publish would suffice only if the sum in question went to the victim. This was true provided that the State, in the exercise of its margin of appreciation, afforded to injured parties other potentially effective remedies that could not be said to restrict in a disproportionate manner the opportunities for obtaining redress for the alleged violations (ibid., § 75).

B. The two aspects (negative and positive) of data protection

70. While the essential object of Article 8 of the Convention is to protect individuals against arbitrary interference by public authorities, or by private bodies to whom responsibilities have been delegated by the State, with their right to respect for their private and family life, home and correspondence, it may also impose on the State certain positive obligations to ensure effective respect for those rights (*Bărbulescu v. Romania* [GC], 2017, § 108).

71. Where a measure interfering with the protection of personal data is taken by an individual or entity purely in the private sector, the Court will examine the case from the standpoint of the State's positive obligations (*Craxi v. Italy (no. 2)*, 2003, §§ 68-76; *Köpke v. Germany* (dec.), 2010; *Alkaya v. Turkey*, 2012, § 32; *Söderman v. Sweden* [GC], 2013, § 89; *Bărbulescu v. Romania* [GC], 2017, § 111; *López Ribalda and Others v. Spain* [GC], 2019, § 111; *Buturugă v. Romania*, 2020, §§ 60-63; *Volodina v. Russia (no. 2*), 2021, §§ 58-68; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, § 111). However, where a measure has been taken by a public entity (*Copland v. the United Kingdom*, 2007, § 39; *Libert v. France,* 2018, § 41; *Drelon v. France*, 2022, § 85) or a private body to which the State has delegated its obligations (*Vukota-Bojić v. Switzerland*, 2016, § 47), the Court will examine the case

from the standpoint of the State's negative obligation. The Court will have to verify that the interference met the requirements of Article 8 § 2, namely that it was in accordance with the law, pursued a legitimate aim and was necessary in a democratic society. This question will be examined in more detail in the part of this guide below on the Three data protection "tests".

72. In the case of *Vukota-Bojić v. Switzerland*, 2016 (§ 47) the Court emphasised that a State could not absolve itself of responsibility under the Convention by delegating its obligations to private bodies or individuals. Given that the private insurance company, which had collected and stored the personal data, was operating the State insurance scheme and that it was regarded by the domestic regime as a public authority, the company had to be regarded as a public authority and acts committed by it were imputable to the respondent State (ibid., § 47).

73. In the case of *Libert v. France,* 2018 (§§ 37-41), the Court dismissed the Government's objection that the National Railway Company (SNCF), the employer of the applicant, who was accused of opening personal files on a work computer, could not be regarded as a public authority for the purposes of Article 8. Even though its staff were employed under private law, the company was a public-law entity, placed under State supervision and having State-appointed directors, thus enjoying an implicit State guarantee.

74. In a case concerning the surveillance of the telephone calls, e-mails and Internet connection of a school employee, the Court took the view that the question to be analysed related to the negative obligation on the State not to interfere with the private life and correspondence of the applicant as the school was a public body for whose acts the Government were responsible for the purposes of the Convention (*Copland v. the United Kingdom*, 2007, § 39).

75. In *Liebscher v. Austria*, 2021, the applicant complained about the obligation to present the entire divorce settlement (rather than an excerpt of it) in order to have his share of real estate transferred to his former wife. The information in the divorce settlement included the names and places of residence of his minor children and former spouse, amount of alimony payments and custody agreements, agreements on separation of assets (other than the real estate) and a list of his income and assets. The transfer of the property, and thus all confirming documents, including the divorce settlement, would be recorded in a land register open to public and which could therefore be consulted by any third person without restriction. The Court approached the case from the standpoint of the State's positive obligation to adopt measures designed to secure respect for private life, including both the provision of a regulatory framework and the implementation, where appropriate, of specific measures (ibid., §§ 60-61).

76. While the boundaries between the State's positive and negative obligations under the Convention do not lend themselves to precise definition, the applicable principles are nonetheless similar. In both contexts regard must be had in particular to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole, subject in any event to the margin of appreciation enjoyed by the State (*Bărbulescu v. Romania* [GC], 2017, § 112).

77. In cases which raise the issue of the protection of personal data, the Court has found that the State's margin of appreciation is broader: where there is no consensus in the member States of the Council of Europe as to the importance of the interest at stake, or the best means of protecting it (*Odièvre v. France* [GC], 2003, § 47; *Breyer v. Germany*, 2020, § 108); where the purely financial data at stake were not closely related to the applicant's identity (*G.S.B. v. Switzerland*, 2015, § 93); and, lastly, in matters of national security (*Leander v. Sweden*, 1987, § 59). By contrast, the margin of appreciation afforded to national authorities was found to be narrower where, for example, personal data subject to automatic processing which considerably facilitated their access and dissemination could harm a person's reputation and render his daily life more difficult (*Khelili v. Switzerland*, 2011, §§ 64, 70). The same consideration is especially valid for the protection of categories of sensitive data, in particular DNA information, which contains the person's genetic make-up and is of great importance

to both the person concerned and his or her family (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 102-103).

78. Inherent positive obligations to ensure the effective protection of the Convention rights and freedoms may involve, for example, an obligation to secure to an individual: access within a reasonable time to information stored systematically about the individual by former State secret services concerning his or her distant past (*Haralambie v. Romania*, 2009, § 79; *Jarnea v. Romania*, 2011, § 50; *Joanna Szulc v. Poland*, 2012, § 87); an "effective and accessible procedure" enabling an interested party to have access to "all relevant and appropriate information" collected and stored by public authorities in order to receive the information necessary to know and to understand the individual's childhood and early development (*Gaskin v. the United Kingdom*, 1989, § 49), to discover his or her personal identity (*Odièvre v. France* [GC], 2003, § 42), or to identify any health risks to which he or she has been exposed (*Guerra and Others v. Italy*, 1998, § 60; *McGinley and Egan v. the United Kingdom*, 1998, § 101; *Roche v. the United Kingdom* [GC], 2005, § 162).

79. The Court has, however, taken the view that such positive obligations are not incumbent on the national authorities in the context of sensitive national security intelligence collected on an individual by the authorities (*Leander v. Sweden*, 1987, § 51).

80. Thus in the case of *Kotilainen and Others v. Finland*, 2020 (§ 83), concerning a school shooting, the Court took the view that the authorities' positive obligation to protect the lives of the applicants' relatives did not extend, under the substantive limb of Article 2, to an obligation for the police to obtain, before the shooting, the perpetrator's medical and military files to verify data on his mental health. Access by the police to an individual's medical data cannot be a matter of routine and must remain subject to specific requirements of necessity and justification.

81. In certain circumstances where the question of personal data arises, for example in the context of particularly serious acts between individuals, the effective enjoyment of Convention rights requires the State to enact specific legislation to protect those rights. Thus in the case of *Söderman v. Sweden* [GC], 2013 (§§ 86-117), the Court found a violation of Article 8 in view of the lack of clear legislative provisions which meant that the isolated act of covert or non-consensual filming/photographing of a naked child went unpunished, a gap in the law that was not compensated for at the time by other criminal-law provisions and having regard to the ineffectiveness of civil remedies (ibid., §§ 108-114). Similarly, in the case of *K.U. v. Finland*, 2008 (§§ 49-50), a violation of Article 8 was found on account of the lack of a legal basis to enable the authorities to oblige an Internet access provider to disclose the identity of a person wanted for placing an indecent advertisement concerning a minor on a dating site. The legislature has to provide the framework for reconciling the various claims which compete for protection in this context. The case of *Khadija Ismayilova v. Azerbaijan*, 2019 (§§ 105-132) concerned the covert recording of a journalist in her home and the public dissemination of the video images. In that case the acts were punishable under the criminal law and a criminal investigation had been opened. The Court nevertheless found that the authorities had not fulfilled their positive obligation to ensure sufficient protection of the applicant's private life by conducting an effective criminal investigation into the very serious interferences with her private life (ibid., §§ 119-131). The case of *Volodina v. Russia (no. 2)*, 2021, § 68, concerned the applicant's complaint that the authorities had failed to protect her against repeated cyberviolence by her partner, who had created fake profiles in her name, had published her intimate photos, had followed her movements, and had sent her death threats via social media. The Court found, in particular, that even though they had the legal tools to prosecute the applicant's partner, the authorities had not conducted an effective investigation and had at no point envisaged taking appropriate measures to protect her. They had thus failed in their duty to protect her against serious abuse.

82. As regards less serious acts between individuals, such as monitoring of employees in the workplace, States may choose whether or not to enact specific legislation concerning video-surveillance (*López Ribalda and Others v. Spain* [GC], 2019, § 113; *Köpke v. Germany* (dec.), 2010) or

the monitoring of employees' non-professional correspondence and communications (*Bărbulescu v. Romania* [GC], 2017, § 119). It is nevertheless for the domestic courts to ensure that any implementation by an employer of surveillance measures interfering with the right of employees to respect for their private life or correspondence is proportionate and accompanied by appropriate and adequate safeguards against abuse (*Köpke v. Germany* (dec.), 2010; *Bărbulescu v. Romania* [GC], 2017, § 120; *López Ribalda and Others v. Spain* [GC], 2019, § 116).

83. In other cases concerning the disclosure of personal data, the Court found that the State had a positive obligation to investigate the alleged violations of Article 8, whether they were committed by private persons or by public authorities. Thus in the case of *Craxi v. Italy (no. 2)*, 2003 (§§ 68-76), concerning the reading-out in court and the disclosure in the press of transcriptions of a politician's telephone conversations, intercepted in the context of criminal proceedings for corruption, the Court took the view that the authorities had a positive obligation to prevent the release into the public domain of the private conversations. As the divulging of the conversations through the press was not a direct consequence of an act of the public prosecutor, but was likely to have been caused by a malfunction of the registry of the domestic court, the Court found a violation of Article 8, as the authorities had failed to take the requisite measures to ensure the effective protection of the applicant's rights by providing appropriate safeguards and conducting an effective investigation.

84. In the case of *Alkaya v. Turkey*, 2012 (§§ 30-40), the Court concluded that the protection given by the domestic authorities to the personal information of a famous actress, whose full address had been disclosed by a newspaper, had been insufficient. Not having found any evidence that appeared capable of justifying on public-interest grounds the newspaper's decision to disclose her address, the Court observed that the domestic courts did not appear to have taken into consideration the possible repercussions on the applicant's life of the publication of her home address in a newspaper. This failure by the domestic courts to assess the competing interests could not be regarded as fulfilling the State's positive obligations under Article 8.

85. In a domestic violence context, the Court found, in *Buturugă v. Romania*, 2020 (§§ 73-78), where the applicant's former husband had abusively consulted her electronic accounts, including Facebook, and had taken copies of her private conversations, documents and photographs, that the authorities had had an obligation to investigate the breach of confidentiality of the applicant's correspondence. The Court, recognising that cyberbullying was recognised as an aspect of violence against women and girls and that it could take on various forms, including cyber violations of privacy, hacking the victim's computer and the stealing, sharing and manipulation of data and images, including intimate details, accepted that such acts as improperly monitoring, accessing and saving the spouse's correspondence could be taken into account by the domestic authorities when investigating cases of domestic violence. Allegations of a breach of confidentiality of one's correspondence required the authorities to conduct an examination on the merits in order to gain a comprehensive grasp of the phenomenon of all the possible forms of domestic violence (ibid., §§ 76-77). As no such examination had taken place, there had been a violation of Article 8.

C. The three data protection "tests"

86. Paragraph 2 of Article 8 indicates the conditions in which there can be an interference with the enjoyment of the protected right; such interference must be "in accordance with the law", must pursue a "legitimate aim" and must be "necessary in a democratic society".

1. Whether the interference was lawful

87. The Court has examined in a number of cases the question whether the requirement, as stated in Article 5 of Convention 108, that personal data undergoing automatic processing must have been obtained and processed fairly and lawfully, has or has not been met. In a number of cases the Court

has found a violation of Article 8 solely on the grounds of a lack of legal basis at national level to authorise measures capable of interfering with the relevant rights (*Taylor-Sabori v. the United Kingdom*, 2002, §§ 17-19; *Radu v. Moldova*, 2014, § 31; *Mockutė v. Lithuania*, 2018, §§ 103-104; *M.D. and Others v. Spain*, 2022, §§ 61-64).

88. In particular, in *Mockutė v. Lithuania*, 2018 (§§ 103-104), the Court noted that neither the Government nor the national courts had indicated any provision that could have formed the legal basis for the communication, by the psychiatric hospital, of information on the health of the applicant, who was an adult, to his mother and to journalists. In *Taylor-Sabori v. the United Kingdom*, 2002 (§§ 17-19), where the applicant had been subjected to police surveillance by the "cloning" of his pager, there existed no statutory system to regulate the interception of pager messages transmitted via a private telecommunications system. In *Radu v. Republic of Moldova*, 2014 (§ 31), the dissemination by a public hospital of medical information on the applicant's pregnancy, state of health and treatment by her employer had not been "in accordance with the law". In *M.D. and Others v. Spain*, 2022 (§§ 61-64), the police drew up a report in respect of judges and magistrates, who exercised their functions in Catalonia and who had signed a manifesto in which they had set out their legal opinion in favour of the possibility of the Catalan people exercising a so-called "right to decide", the report revealing the personal data, photographs, professional information and political views of some of them. The Court observed that the drawing up of the report by the police had not been provided for by law, and since the public authorities had used the personal data for a purpose other than that which justified collection, the mere existence of the police report, which had been drafted in respect of individuals whose behaviour had not implied any criminal activity, amounted to a violation of Article 8 of the Convention.

89. In other cases the Court found a violation of Article 8 on the ground that domestic law, which was supposed to protect personal data, was inaccessible or confidential (*Vasil Vasilev v. Bulgaria*, 2021, §§ 169-170; *Nuh Uzun and Others v. Turkey*, 2022, §§ 80-99) or was not sufficiently clear and foreseeable (*Vukota-Bojić v. Switzerland*, 2016; *Ben Faiza v. France*, 2018, §§ 58-61; *Benedik v. Slovenia*, 2018*; Rotaru v. Romania* [GC], 2000; *Zoltán Varga v. Slovakia*, 2021, § 162; *Haščák v. Slovakia,* 2022, §§ 94-95). Thus in *Nuh Uzun and Others v. Turkey*, 2022, §§ 80-99, prisoners' correspondence was scanned and uploaded onto the National Judicial Network Server on the basis of instructions issued by the Ministry of Justice, directly and specifically addressed to the public prosecutors and prison authorities, which had not been made accessible to the public in general or to the applicants in particular. In the case of *Vukota-Bojić v. Switzerland*, 2016, §§ 71-77, the provisions forming the basis of the covert surveillance to which the applicant had been subjected by her insurance company after a road accident had not indicated with sufficient clarity the scope and manner of exercise of the discretion conferred on insurance companies acting as public authorities in insurance disputes to conduct secret surveillance of insured persons. In the case of *Rotaru v. Romania* [GC], 2000 (§§ 57-62), concerning personal information held by the Romanian intelligence service, national law did not define the type of information which could be processed, the categories of individuals in respect of whom surveillance measures could be taken and in what circumstances, or the procedure to be followed. In *Benedik v. Slovenia*, 2018 (§ 132), certain legal provisions used by the police to obtain data on a subscriber associated with a dynamic IP address lacked clarity and provided no protection against arbitrary interference, as there were no safeguards against abuse or any independent monitoring of the police powers in question.

90. By contrast, in other cases the Court found no violation of Article 8 after finding that the domestic law was clear and foreseeable and afforded sufficient safeguards against potential abuse (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 154; *Ben Faiza v. France*, 2018, § 75). In *Ben Faiza v. France*, 2018 (§§ 70-76), a court order used to obtain, from a mobile telephone service provider, personal information on the applicant which did not concern the content of the calls, had been "in accordance with the law". Such court orders were authorised and governed by the relevant statutory framework and there were also safeguards against arbitrariness, as such orders had to be

authorised beforehand by a prosecutor on pain of nullity and were subject to judicial review, and the information obtained could be excluded from evidence in the event of any illegality (ibid., § 73).

91. The Court reached a similar conclusion in *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 (§ 154), concerning a decision by the Data Protection Board, endorsed by the courts, prohibiting the widespread publication of tax data. The wording of the relevant data protection legislation and the way in which it had been applied following guidance given to the Finnish courts by the Court of Justice of the European Union (CJEU), had been sufficiently foreseeable. Even though the case was the first of its kind under the Personal Data Act and the Supreme Administrative Court had sought guidance from the CJEU on the interpretation of the derogation in the Data Protection Directive, that did not render the domestic courts' interpretation and application of the journalistic derogation arbitrary or unpredictable (ibid., § 150). Since the applicant companies were media professionals they should, as such, have been aware of the possibility that the mass collection of data and its wholesale dissemination might not be considered as processing "solely" for journalistic purposes under the relevant provisions of Finnish and EU law (ibid., § 151).

92. Lastly, in other cases the Court has found that the requirement for interference to be "in accordance with the law" was so closely linked to the "necessary in a democratic society" criterion that the two conditions had to be discussed together (*S. and Marper v. the United Kingdom* [GC], 2008, § 99; *Kvasnica v. Slovakia*, 2009, § 84; *Kennedy v. the United Kingdom*, 2010, § 155).

93. In the specific context of covert surveillance measures, such as the interception of communications, the Court has found that "foreseeability" cannot be understood in the same way as in many other fields. In its view, it cannot mean that an individual should be able to foresee when the authorities are likely to have recourse to such measures so that he or she can adapt his or her conduct accordingly (*Adomaitis v.Lithuania*, 2022, § 83). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on covert surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which, and the conditions upon which, public authorities are empowered to resort to any such measures (*Malone v. the United Kingdom,* 1984, § 67; *Leander v. Sweden*, 1987, § 51; *Valenzuela Contreras v. Spain,* 1998, § 46; *Weber and Saravia v. Germany* (dec.), 2006, § 93; *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007, § 75; *Roman Zakharov v. Russia* [GC], 2015, § 229). In addition, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (*Roman Zakharov v. Russia* [GC], 2015, § 230).

94. In its case-law on the interception of communications in the context of criminal investigations, the Court has determined that, in order to prevent abuse of power, the law must at least set out the following six elements: the nature of the offences that may give rise to an interception order; the definition of the categories of persons whose communications may be intercepted; the time-limit on the implementation of the measure; the procedure to be followed for the examination, use and storage of the data collected; the precautions to be taken for the transmission of the data to other parties; and the circumstances in which intercept data may or must be deleted or destroyed (*Huvig v. France*, 1990, § 34; *Valenzuela Contreras v. Spain,* 1998, § 46; *Weber and Saravia v. Germany* (dec.), 2006, § 95; *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007, § 76). In *Roman Zakharov v. Russia* [GC], 2015 (§ 238), it confirmed that these same minimum safeguards also applied in cases where the interception had been implemented on national security grounds; however, in order to determine whether or not the impugned legislation was incompatible with Article 8, the Court also took account of the following factors: the arrangements for supervising

the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law[3].

95. In the context of personal data collected by the authorities and stored in databases for purposes related to the prevention or punishment of crime, the Court has indicated that it is essential to have clear, detailed rules governing the scope and application of such measures, together with minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 99, 103; *Nuh Uzun and Others v. Turkey*, 2022, § 86). The Court has found a violation of Article 8 in cases where the domestic law did not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities (*Shimovolos v. Russia*, 2011, § 70 ; *Dimitrov-Kazakov v. Bulgaria*, 2011, § 33). In the case of *Shimovolos v. Russia*, 2011 (§ 69), the creation and maintenance of a surveillance database storing personal data, including on the movements of a human rights activist, and the procedure for its operation, were governed by a ministerial order which had never been published or otherwise made accessible to the public. In the case of *Dimitrov-Kazakov v. Bulgaria*, 2011 (§ 33), the registration of an individual as an "offender" in the police registers was based on a non-public instruction at the material time which was confidential in character and was reserved, until its subsequent declassification, for the internal use of the Interior Ministry.

96. In the case of *Catt v. the United Kingdom*, 2019 (§§ 97, 106), the Court emphasised the risk of ambiguity in the legal basis used by the authorities for the collection and retention of personal data, stemming from loosely defined notions in domestic law.

2. Whether the interference pursued a legitimate aim

97. In a number of cases the Court has examined whether the requirement, as stated in Article 5 of Convention 108, that personal data undergoing automatic processing must have been collected for explicit, specified and legitimate purposes, has or has not been met. In these cases, the examination of the legitimate aims which may justify interference with the exercise of the Article 8 rights, as listed in paragraph 2, is rather succinct. These aims are the protection of national security, public safety and the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. The Court generally confirms the existence of one or more of these legitimate aims invoked by the Government.

98. The Court has taken the view, for example, that the storage in a secret police register of data on the private life of individuals, then the use of that data in the vetting of candidates for posts of importance for national security, pursued a legitimate aim for the purposes of Article 8, namely the protection of national security (*Leander v. Sweden*, 1987, § 49). Surveillance of an applicant by GPS, ordered by a prosecutor for an investigation into several acts of attempted murder for which a terrorist movement had claimed responsibility and to prevent further bomb attacks, had in the Court's view served the interests of national security and public safety, the prevention of crime and the protection of the rights of the victims (*Uzun v. Germany,* 2010, § 77).

99. The Court also found that the transmission of banking data to the authorities of another State under a bilateral agreement pursued a legitimate aim, as the measure served to protect the country's economic well-being (*G.S.B. v. Switzerland*, 2015, § 83). Given that the banking sector was an economic branch of great importance to the respondent State, the impugned measure, which formed

[3] See also Guide to Article 8 of the Convention (right to respect for private and family life) about the requirement of the foreseeability of the law in matters of interception of communications, telephone tapping and covert surveillance.

part of an all-out effort by the Swiss Government to settle the conflict between a bank (described as "a major player in the Swiss economy employing a large number of persons") and the US tax authorities, the measure could validly be considered conducive to protecting the country's economic well-being (ibid., § 83).

100. Referring to international instruments under which fairness and equality of opportunity were fundamental to the fight against doping, the Court found that the protection of health and morals justified the obligation to establish the whereabouts of athletes, having regard to the need to tackle doping in sport (*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, 2018, §§ 164-166). In the Court's view, what the Government had described as "morals", in the context of efforts to ensure equal and meaningful competition in sports, was also linked to the legitimate aim of "protection of the rights and freedoms of others", since the use of doping agents in order to gain an advantage over other athletes was a dangerous incitement to amateur athletes, and in particular young people, to follow suit in order to enhance their performance, and deprived spectators of the fair competition which they were entitled to expect (ibid., § 166).

101. In the case of *Ben Faiza v. France*, 2018 (§ 77), the Court found that a court order used to obtain, from a mobile telephone service provider, personal information on the applicant which did not concern the content of the calls, had sought to establish the truth in the context of criminal proceedings for the importing of drugs in an organised gang, criminal conspiracy and money laundering. The measure had thus pursued the legitimate aims of preventing disorder or crime or protecting public health.

102. The interception of telephone conversations of the applicant – a prison director, who had been suspected of corruption – the storage of that information and its disclosure in the disciplinary proceedings, which ultimately had led to his dismissal, were found to aim at preventing acts of a corrupt nature and guaranteeing the transparency and openness of public service, and thus had pursued the legitimate aims of the prevention of disorder or crime, and the protection of the rights and freedoms of others in *Adomaitis v. Lithuania*, 2022 (§ 84).

103. In the case of *López Ribalda and Others v. Spain* [GC], 2019 (§§ 118, 123), the legitimate interest for the employer in taking measures in order to find out and punish the person(s) responsible for suspected thefts, with the aim of ensuring the protection of the company's property and its smooth operation, could justify measures involving the video-surveillance of employees in the workplace.

3. Whether the interference was "necessary in a democratic society"

104. In order to be necessary in a democratic society, any measure interfering with the protection of personal data under Article 8 must meet a "pressing social need" and must not be disproportionate to the legitimate aims pursued (*Z v. Finland*, 1997, § 94; *Khelili v. Switzerland*, 2011, § 62; *Vicent Del Campo v. Spain*, 2018, § 46). The reasons invoked by the Government must be pertinent and sufficient (*Z v. Finland*, 1997, § 94). While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention (*S. and Marper v. the United Kingdom* [GC], 2008, § 101).

105. In the context of particularly serious acts between individuals capable of interfering with Article 8 rights, the Court's review of whether they met the requirement of being "necessary in a democratic society" concerns the manner in which the State has enacted specific legislation to ensure sufficient protection of those rights (*K.U. v. Finland*, 2008, §§ 43-50; *Söderman v. Sweden* [GC], 2013, §§ 80-83). As to less serious acts between individuals, such as video-surveillance of employees in the workplace, the Court's review of whether the measure was "necessary in a democratic society" will concern the manner in which the domestic courts have taken into consideration the criteria that the Court has established in its case-law, thus showing whether the competing interests have been weighed in the balance (*López Ribalda and Others v. Spain* [GC], 2019, §§ 116-117, § 122). In reviewing those criteria,

if one is found to be lacking the safeguards deriving from the others will be all the more important and may sufficiently compensate for that failure (ibid., § 131).

106. Generally speaking, in order to ascertain whether or not a measure interfering with the protection of personal data under Article 8 fulfils the condition of being "necessary in a democratic society", the Court has examined whether it has complied with the requirements listed in Article 5 of Convention 108, namely and in particular, the requirement to minimise the amount of data collected, to ensure that they are accurate, adequate, relevant and not excessive in relation to the purposes for which they are processed, to limit the duration of their storage, to use them for the purposes for which those data have been collected and to ensure transparency in their processing.

a. Requirement to minimise the amount of data collected or recorded

107. In a number of cases the Court has examined the question whether the personal data undergoing automatic processing had been adequate, relevant and not excessive in relation to the purposes for which they had been recorded (*L.L. v. France*, 2006, §§ 45-46; *Vicent Del Campo v. Spain*, 2018, § 51; *Khadija Ismayilova v. Azerbaijan*, 2019, § 147; *Kruglov and Others v. Russia*, 2020, § 132 *in fine*).

108. The Court found a violation of Article 8: after noting that, as regards data held on the applicants' electronic devices which had been seized, it did not seem that any sort of sifting procedure to minimise the quantity of that data had been followed during the searches (*Kruglov and Others v. Russia*, 2020, § 132 *in fine*); as regards a court decision identifying the applicant, who was not a party to the proceedings, as having committed acts of harassment in the workplace, whereas the judge could have refrained from naming him, or could have referred to him simply by his initials, in order to avoid stigmatisation (*Vicent Del Campo v. Spain*, 2018, § 51); in a case where the personal data of a journalist, who had been filmed without her knowledge in the intimacy of her home, had been disclosed, in a manner considered excessive and pointless, in an investigation progress report (*Khadija Ismayilova v. Azerbaijan*, 2019, § 147).

109. In the Court's view, the compilation of databases in order to contribute to the prevention and punishment of certain offences cannot be implemented in an excessive drive to maximise the information stored in them (*B.B. v. France*, 2009, § 62; *Gardel v. France*, 2009, § 63; *M.B. v. France*, 2009, § 54). Without respect for the requisite proportionality *vis-à-vis* the legitimate aims assigned to such mechanisms, their advantages would be outweighed by the serious breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction (*M. K. v. France*, 2013, § 35 ; *Aycaguer v. France*, 2017, § 34). In the context of a scheme of indiscriminate and indefinite retention, the argument that "the more data is retained, the more crime is prevented" would in practice be tantamount to justifying the storage of information on the whole population and their deceased relatives, which would most definitely be excessive and irrelevant (*Gaughran v. the United Kingdom*, 2020, § 89).

110. In the case of *Catt v. the United Kingdom*, 2019 (§ 122), the lack of effective safeguards to ensure the destruction, in a police database, of personal information disclosing the political opinions of a peaceful protester, once its retention became disproportionate, had entailed a violation of Article 8.

b. Requirement of accuracy and updating of data

111. The Court has heard a number of cases about the storage by the authorities of data which proved inaccurate or whose accuracy was disputed by the data subject (*Cemalettin Canlı v. Turkey*, 2008, §§ 34-37, about inaccurate police files in criminal proceedings; *Rotaru v. Romania* [GC], 2000, § 36, about an individual's inability to contest information collected by security services concerning his alleged participation in a "legionnaire" movement in his distant past).

112. False or incomplete personal information collected and retained by the authorities may make the data subject's daily life more difficult (*Khelili v. Switzerland*, 2011, § 64), may prove defamatory

(*Rotaru v. Romania* [GC], 2000, § 44) or may remove certain statutory procedural safeguards to protect the data subject's rights when such data can be transmitted between various authorities (*Cemalettin Canlı v. Turkey*, 2008, §§ 42-43). The Court furthermore emphasised that it was inappropriate to collect personal data on the basis of mere speculation or presumption without any proven factual basis (*Drelon v. France*, 2022, § 97).

113. In the Court's view, it is the authorities' task to prove the accuracy of data which has been stored. In the case of *Khelili v. Switzerland*, 2011 (§§ 66-70), where uncertainties surrounded a vague and general allegation of unlawful prostitution recorded by the authorities, the retention of the word "prostitute" in the police files for years had not been "necessary in a democratic society", taking account of the contradictory behaviour of the authorities, the principle that it was a matter for those same authorities to prove the accuracy of particular data, the narrow margin of appreciation enjoyed by the domestic authorities in that area and the seriousness of the interference with the applicant's right to respect for her private life under Article 8. Likewise, in *Drelon v. France*, 2022, §§ 95-97, concerning the refusal by the French Blood Donation Service to accept the applicant as a blood donor based on his presumed homosexuality, the Court observed that the collection of personal data should have a precise and accurate factual basis, whereas in the present case a conclusion about the applicant's sexual practices had been made only because he had refused to answer the questions about his sex life during the pre-donation medical interview.

114. In the case of *Anchev v. Bulgaria* (dec.), 2017 (§§ 112-115), where the applicant had been the subject of three investigations and had been flagged, on the basis of archive material, as a collaborator of the former security services under a law on the disclosure of civil servants who had collaborated with the Communist regime, the Court dismissed the applicant's complaint after noting that he had been able to consult the archives and then publicly contest their accuracy on a concrete basis.

c. Requirement that data be retained for no longer than is necessary to fulfil the purpose for which they were recorded[4]

115. The question of the need to limit the duration of personal data retention has been examined by the Court in a number of cases (*S. and Marper v. the United Kingdom* [GC], 2008; *B.B. v. France*, 2009; *Gardel v. France*, 2009; *M.B. v. France*, 2009; *M.K. v. France*, 2013; *J.P.D. v. France* (dec.), 2014; *Peruzzo and Martens v. Germany* (dec.), 2013; *W. v. the Netherlands* (dec.), 2009; *Brunet v. France*, 2014; *Drelon v. France*, 2022, § 98). A maximum retention period of thirty years in the national judicial database of sex offenders from the end of a prison sentence lasting between five and fifteen years for the offence of rape committed against a minor was not considered disproportionate to the legitimate aim pursued by the data storage, namely the prevention of disorder or crime (*B.B. v. France*, 2009, §§ 67-68; *Gardel v. France*, 2009, §§ 68-69; *M.B. v. France*, 2009, §§ 59-60).

116. However, the permanent retention in a national database of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, regardless of the nature or seriousness of the offence of which the person had originally been suspected, and regardless of age, was found to breach Article 8 (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 125-126). The permanent retention of an unconvicted person's data may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society (ibid., § 124).

117. The lack of a maximum time-limit for the retention of personal data is not necessarily incompatible with Article 8 (*Gaughran v. the United Kingdom*, 2020, § 88; *Peruzzo and Martens v. Germany* (dec.), 2013, § 46), but procedural safeguards will be all the more necessary where the

[4] See also the part below of the present guide on the Data retention period.

storage of data depends entirely on the authorities' diligence in ensuring that its duration is proportionate (ibid., § 46; *Aycaguer v. France*, 2017, §§ 44-46).

d. Requirement to limit the use of data to the purpose for which they were recorded

118. The Court has taken the view that it is important to limit the use of data to the purpose for which they were recorded. Thus in the case of *Karabeyoğlu v. Turkey*, 2016 (§§ 112-121), the use in a disciplinary investigation of data that came from telephone tapping during a criminal investigation, and thus for a different purpose from that which had justified their collection, was found to breach Article 8.

119. In the case of *Surikov v. Ukraine*, 2017 (§§ 83-95), the long-term retention of data concerning an individual's mental health, together with their dissemination and use for purposes that were unconnected with the reasons which had initially justified their collection, had constituted a disproportionate interference with the data subject's right to respect for his private life.

120. The question of the risk of improper use of personal information also arose in the case of *K.H. and Others v. Slovakia*, 2009 (§§ 45-57), where the applicants, eight ethnic Roma women suspected of being sterilised during a hospital stay, complained that they had been unable to obtain copies of their medical record. The Court found a violation of Article 8, pointing out that the risk of abuse alleged by the Government could have been prevented by means such as incorporation in domestic law of appropriate safeguards with a view to strictly limiting the circumstances under which such data could be disclosed and the scope of persons entitled to access the files (ibid., § 56).

121. In order to establish the boundary of the intimacy of private life secured by Article 8, the Court has made a distinction between surveillance of an individual's acts in a public place for security purposes, and recordings of such acts used for other purposes, going beyond what the individual concerned could have expected (*Peck v. the United Kingdom*, 2003, §§ 59-62, on the filming of an applicant in a public place on security grounds where the footage was disclosed to the media; *Perry v. the United Kingdom*, 2003, §§ 41-42, on a subterfuge used by the police for the purposes of identifying the applicant by video recording, going beyond the limits of the normal or foreseeable use of surveillance cameras in police stations).

e. Requirement of transparency of data processing procedures[5]

122. In a series of cases concerning personal data collected and stored by public authorities, the Court found that the authorities had a positive obligation to provide those concerned with an "effective and accessible procedure" to allow them to have access to "all relevant and appropriate information" that was necessary, for example, to know and to understand their childhood and early development (*Gaskin v. the United Kingdom*, 1989, § 49), to discover their personal identity (*Odièvre v. France* [GC], 2003, §§ 41-49), to identify any health risks to which they had been exposed (*Roche v. the United Kingdom* [GC], 2005, § 162; *Guerra and Others v. Italy*, 1998, § 60; *McGinley and Egan v. the United Kingdom*, 1998, § 101), or to retrace their personal history during a former totalitarian regime (*Haralambie v. Romania*, 2009, § 93).

123. This requirement of transparency will be less stringent in the context of information that is sensitive for national security (*Leander v. Sweden*, 1987, § 51; *Segerstedt-Wiberg and Others v. Sweden*, 2006, § 102; *Dalea v. France* (dec.), 2010).

[5] See also the part below of the present guide on the Right of access to one's own data.

II. Data protection and the right to respect for private life (Article 8 of the Convention)

Article 8 of the Convention

"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 is 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."

124. The Court has to date dealt with a large number of personal data operations conducted by the authorities or various privates agencies, assessing whether the data subject's "private life", "home" and/or "correspondence" were infringed in a manner incompatible with Article 8. In different contexts it has specified the scope of a number of rights on which legal and natural persons can rely in order to protect their personal data.

A. Data operations liable to infringe the right to respect for private life

125. With the development of technologies, data collection, storage and disclosure are taking on a wide variety of forms. In several cases the Court has considered whether one or more of these operations had resulted in an unjustified interference with the data subject's right to respect for his or her private life.

1. Personal data collection

126. The Court has examined personal data collection operations in a variety of contexts: as regards action to combat organised crime and terrorism by means of different secret surveillance systems created by the authorities; in the judicial context concerning personal data collected by the authorities for use in evidence; in the health context; in the context of data collected on the workplace, covering both public-sector and private-sector employers; and finally, in the context of legal obligations on public or private bodies to transmit to the authorities personal data in their possession in order to protect a general public interest.

a. Data collection by the authorities via covert surveillance[6]

127. The Court has dealt with a considerable number of cases concerning the issue of personal data collection by means of various methods of secret surveillance. Whatever surveillance system the authorities use, the existence of adequate and sufficient guarantees against abuse is essential. The Court considers that powers of secret surveillance of citizens are tolerable only in so far as strictly necessary for safeguarding the democratic institutions (*Klass and Others v. Germany*, 1978, § 42; *Szabó and Vissy v. Hungary*, 2016, §§ 72-73). Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued (*Segerstedt-Wiberg and Others v. Sweden*, § 88). Domestic legislation must provide safeguards that are sufficiently

[6] See also Guide to Article 8 of the Convention (right to respect for private and family life).

precise, effective and comprehensive in respect of the ordering and execution of surveillance measures and for the securing of potential redress (*Szabó and Vissy v. Hungary*, 2016, § 89).

i. Telephone tapping and metering

128. In the judicial framework, the Court has found violations of Article 8 in the following spheres: phone tapping and supply of records of metering to the police (list of telephone numbers called) (*Malone v. the United Kingdom*, 1984, §§ 63-89); monitoring and transcription of all the applicants' commercial and private phone calls (*Huvig v. France*, 1990, §§ 24-35); monitoring and recording of several of the applicant's phone conversations by tapping a third party's telephone line (*Kruslin v. France*, 1990, §§ 25-36); phone tapping of a person via a third party's telephone line (*Lambert v. France*, 1998, §§ 21-41); monitoring and recording by the public prosecutor of a telephone call received by an individual in his office from another individual in the then Soviet Embassy in Bern (*Amann v. Switzerland* [GC], 2000, §§ 45-62); phone tapping in the framework of a preliminary investigation (*Prado Bugallo v. Spain,* 2003, §§ 28-33); telephone conversations monitored in the context of a criminal prosecution and subsequently published in the press (*Craxi v. Italy (no. 2)*, 2003, §§ 57-84); inclusion in the applicant's case file of a transcription from phone tapping carried out in proceedings in which he had not been involved (*Matheron v. France*, 2005, §§ 27-44); monitoring of phone calls by the authorities in the absence of authorisation by the public prosecutor issued in the name of the suspect and without legislation providing sufficient safeguards against arbitrariness (*Dumitru Popescu v. Romania (no. 2)*, 2007, §§ 61-86); tapping of phone calls made by a lawyer for criminal investigations (*Kvasnica v. Slovakia*, 2009, §§ 80-89); insufficient safeguards against arbitrariness in domestic provisions on phone tapping (*Dragojević v. Croatia*, 2015, §§ 85-102; *Liblik and Others v. Estonia*, 2019, §§ 132-143); lack of adequate judicial guarantees (*Moskalev v. Russia*, 2017, §§ 35-45); lack of effective supervision of the recoding of phone calls in the framework of criminal proceedings (*Pruteanu v. Romania*, 2015, §§ 41-58); monitoring of mobile phone calls (*Šantare and Labazņikovs v. Latvia*, 2016, §§ 56-63); unjustified failure to provide *ex post* notification of a temporary mobile phone tapping measure (*Cevat Özel v. Turkey,* 2016, §§ 29-37); and preventive monitoring of phone calls (*Mustafa Sezgin Tanrıkulu v. Turkey,* 2017, §§ 45-66); the practically unlimited power of the intelligence services in carrying out surveillance of an individual and of meetings held in the flat that he owned without sufficient legal safeguards (*Zoltán Varga v. Slovakia*, 2021, §§ 170-171), which also randomly affected another person without any protection being provided under domestic law for such a person (*Haščák v. Slovakia,* 2022, § 95); and the interception, recording and transcription of a telephone conversation between a lawyer and one of his clients, a former defence minister, who was under covert surveillance in connection with a criminal investigation (*Vasil Vasilev v. Bulgaria*, 2021, §§ 167-181).

129. The Court found no violation of Article 8 concerning phone tapping which had been authorised by judicial decision, in the knowledge that the necessity of that measure had been assessed by the courts (*İrfan Güzel v. Turkey*, 2017, §§ 78-89).

130. The Court also found no violation of Article 8 in the following cases: the registration by the police of telephone numbers called by an individual by metering his private telephone (*P.G. and J.H. v. the United Kingdom*, 2001, §§ 42-51); the tapping of a judge's telephone lines in the framework of criminal investigations into an illegal organisation of which he had been suspected of being a member, contributor or supporter (*Karabeyoğlu v. Turkey*, 2016, §§ 74-111); and the interception of telephone communications of a prison director in the context of a criminal investigation into his suspected corruption-related activity in the prison for personal gain, even though eventually that investigation was discontinued on the basis of a lack of incriminating evidence (*Adomaitis v. Lithuania*, 2022, §§ 81-90).

131. Several applications have been declared inadmissible as manifestly ill-founded, as regards: phone tapping in the framework of preventive intelligence activities by the police (*Deveci v. Türkiye* (dec.), 2022); phone tapping in the framework of a preliminary investigation (*Greuter v. the*

Netherlands (dec.), 2002); phone tapping in the framework of a criminal investigation as one of the main investigative methods helping to prove the involvement of certain individuals in a major drug-trafficking network (*Coban v. Spain* (dec.), 2006); and monitoring of telephone communications effected by a Member of the European Parliament charged with misappropriation of corporate assets, and the inapplicability in that case of the special treatment given to national MPs (*Marchiani v. France* (dec.), 2008).

132. In the prison context, the illegal recording and storage of a prisoner's telephone calls by the prison authorities, and their subsequent use in evidence to convict the prisoner of a further offence, had breached Article 8, in the case of *Doerga v. the Netherlands*, 2004 (§§ 43-54).

133. In a range of other fields the Court has found violations of Article 8 concerning: an automatic system of monitoring all correspondence and telephone calls by minors housed in a correctional boarding school, ruling out any kind of confidentiality as regards the types of exchanges monitored (*D.L. v. Bulgaria*, 2006, §§ 100-116); the warranted interception by the Ministry of Defence of outgoing communications by organisations working in the civil liberties field (*Liberty and Others v. the United Kingdom*, 2008, §§ 56-70); the mere existence of legislation allowing the monitoring of telecommunications by a Moldavan non-governmental organisation specialising in representing applicants before the Court (*Iordachi and Others v. Moldova*, 2009, §§ 29-54); leaks to the media and broadcasting of a private conversation recorded with the authorities' approval on the telephone line of a politician who was under investigation by the prosecuting authorities (*Drakšas v. Lithuania*, 2012, § 62); shortcomings in the legal framework governing secret monitoring of mobile phone calls put in place by mobile phone network operators, enabling the Federal Security Service to intercept any kind of telephone communication without prior judicial authorisation (*Roman Zakharov v. Russia* [GC], 2015, §§ 163-305); the use in a disciplinary inquiry of phone tapping data from a criminal investigation (*Karabeyoğlu v. Turkey*, 2016, §§ 112-121); and the use in disciplinary proceedings against a lawyer of a transcription of a conversation with one of her client's whose phone had been tapped (*Versini-Campinchi and Crasnianski v. France*, 2016, §§ 49-84). Conversely, the use in disciplinary proceedings against a prison director of information received as a result of phone tapping carried out in the context of a criminal investigation into his suspected corruption was found to be proportionate (*Adomaitis v. Lithuania*, 2022, § 87).

ii. Interception of pager messages

134. In the case of *Taylor-Sabori v. the United Kingdom*, 2002, §§ 18-19, in the framework of judicial proceedings, the interception of the applicant's pager messages by the police and the subsequent reference to them as the basis for a conviction were deemed contrary to Article 8 in the absence of any legal regulations on such interception.

iii. Audio-surveillance and video-surveillance

135. The Court found a violation of Article 8 in a case where the recording of a conversation using a radio-transmission device in the framework of a secret police operation had not been accompanied by proper procedural safeguards (*Bykov v. Russia* [GC], 2009, §§ 81, 83; *Oleynik v. Russia*, 2016, §§ 75-79).

136. The Court has drawn a distinction between the monitoring of an individual's acts in a public place for security purposes and the recording of those acts for other purposes, going beyond what the person could possibly have foreseen (*Peck v. the United Kingdom*, 2003, §§ 59-62; *Perry v. the United Kingdom*, 2003, §§ 41-42), in order to establish the strict boundary of private life as secured under Article 8 in the sphere of secret surveillance measures and the interception of communications by the State authorities.

137. In the judicial framework, the Court has found breaches of Article 8 in the following cases: recording of the applicants' voices when they were being charged and while they were being held in

their cells at the police station (*P.G. and J.H. v. the United Kingdom*, 2001, §§ 56-63); the filming, for identification purposes, of a suspect in a police station using a covert closed-circuit camera (*Perry v. the United Kingdom*, 2003, §§ 36-49); the recording by the police, by means of a listening device installed in the home of a third person whom the applicant had visited, of an unprompted, spontaneous conversation during which the applicant had admitted that he had been a party to the importation of drugs (*Khan v. the United Kingdom*, 2000, §§ 25-28); police bugging of private premises in the framework of a judicial investigation (*Vetter v. France*, 2005, §§ 20-27); recording of a conversation by means of a listening device planted on the person by the police authorities, and the subsequent use of that recording at the trial, albeit not as the only item of incriminating evidence (*Heglas v. Czech Republic*, 2007, §§ 71-76); and the recording of communications by an individual in the context and for the benefit of an official investigation, whether criminal or of another nature, with the co-operation and technical assistance of the State investigative authorities (*Van Vondel v. the Netherlands*, 2007, §§ 47-55).

138. In the prison context, the Court has found violations of Article 8 in the following cases: the use by the authorities of video and audio recording devices covertly installed in the applicant's cell and in the prison visiting area, as well as on the person of a fellow-prisoner, facilitating the recording of non-spontaneous, prompted statements by the applicant (*Allan v. the United Kingdom*, 2002, §§ 35-36); the recording of conversations between prisoners and their families in prison visiting rooms (*Wisse v. France*, 2005, §§ 28-34); secret surveillance of a prisoner's consultations with his legal adviser (*R.E. v. the United Kingdom*, 2015, §§ 115-143); and round-the-clock video surveillance of prisoners in their cells by means of a covert closed-circuit camera (*Gorlov and Others v. Russia*, 2019, §§ 83-100).

139. The Court found no violation of Article 8 concerning covert surveillance of a prisoner's consultations with the person appointed to assist him as a vulnerable person after his arrest (*R.E. v. the United Kingdom*, 2015, §§ 154-168). The provisions concerning directed surveillance, insofar as they related to the possible surveillance of consultations between detainees and appropriate adults, had been accompanied by adequate safeguards against abuse.

140. In different contexts where the data in question had been collected via hidden cameras, the Court has found violations of Article 8 concerning: transmission to the media of a video from a hidden closed-circuit camera filming a person attempting to commit suicide in a public place (*Peck v. the United Kingdom*, 2003, §§ 57-87); TV broadcasting of an unpixellated and unblurred image of an individual taken by a hidden camera (*Bremner v. Turkey*, 2015, §§ 71-85); covert video recording of a journalist at home and public broadcasting of the videos (*Khadija Ismayilova v. Azerbaijan*, 2019, §§ 108-132). See also paragraphs 232 to 234 and 152 to 157 of this guide.

iv. Geolocation of vehicle by GPS[7]

141. In the case of *Uzun v. Germany*, 2010 (§§ 49-81) the GPS surveillance of an individual suspected of terrorism had not amounted to a breach of Article 8. Conversely, in *Ben Faiza v. France*, 2018 (§§ 53-61), the installation of a geolocation device in a vehicle and the use of the data obtained thereby, providing the investigators with real-time information on the applicant's movements and enabling them to arrest him, were deemed contrary to Article 8.

v. Surveillance by private detectives

142. In the case of *Vukota-Bojić v. Switzerland*, 2016 (§§ 52-78), the Court found a violation of Article 8 in respect of the unlawful surveillance by private detectives of the activities of a person in receipt of disputed social welfare benefits. Domestic law had not indicated with sufficient clarity the scope and

[7] See also the section of the Guide above on GPS location data.

manner of exercise of the discretion conferred on insurance companies acting as public authorities in insurance disputes to conduct secret surveillance of insured persons.

vi. Monitoring of correspondence

143. In the prison context, the Court found violations of Article 8 concerning: the interception and opening of a prisoner's correspondence (*Lavents v. Latvia*, 2002, §§ 136-137); the opening of a prisoner's correspondence, including in the case of a malfunctioning of the mail service within the prison (*Demirtepe v. France*, 1999, §§ 26-28; *Valašinas v. Lithuania*, 2001, §§ 128-130); the interception and censorship of a prisoner's correspondence (*Silver and Others v. the United Kingdom*, 1983, §§ 84-105; *Labita v. Italy* [GC], 2000, §§ 176-184; *Niedbała v. Poland*, 2000, §§ 78-84; *Messina v. Italy (no. 2)*, 2000, §§ 78-83); interception of prisoners' letters to their lawyer (*Ekinci and Akalın v. Turkey*, 2007, §§ 37-48); interception of prisoners' correspondence with their lawyers and with the European Commission of Human Rights (*Campbell v. the United Kingdom*, 1992, §§ 32-54; *A.B. v. the Netherlands*, 2002, §§ 81-94); opening of letter sent to a prisoner by the Commission (*Peers v. Greece*, 2001, §§ 81-84); surveillance of a prisoner's correspondence with his consultant (*Szuluk v. the United Kingdom*, 2009, §§ 47-55); the practice of scanning and uploading prisoners' private correspondence, both incoming and outgoing, onto the National Judicial Network Server (*Nuh Uzun and Others v. Turkey*, 2022, §§ 80-99). Conversely, in the case of *Erdem v. Germany*, 2001 (§§ 53-70), no violation of Article 8 was found with regard to the interception of correspondence between a prisoner suspected of terrorism and his lawyer.

144. In a different context, a violation of Article 8 was found in a case where a bankrupt's correspondence was opened and copied to file by the Trustee in Bankruptcy (*Foxley v. the United Kingdom*, 2000, §§ 27-47).

vii. Covert surveillance, espionage and mass surveillance operations

145. In the case of *Roman Zakharov v. Russia* [GC], 2015 (§§ 171-172) the Court ruled that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures or of legislation permitting such measures, if certain conditions are satisfied, and that the approach adopted in *Kennedy v. the United Kingdom*, 2010 (§ 124) was best suited to the need to ensure that the secrecy of surveillance measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court. In the case of *Ekimdzhiev and Others v. Bulgaria*, 2022 (§ 262-277 and 371-384) the Court accepted, on the basis of the principles developed in *Roman Zakharov v. Russia* [GC], 2015 (§ 171), that the applicants, two lawyers and two non-governmental organisations related to them, may claim to be victims of an interference with their rights under Article 8 owing to the mere existence of domestic law or practices permitting secret surveillance as well as laws governing the accessing of retained communications data by the authorities.

146. The Court found violations of Article 8 in the following cases: where the applicant association could be subjected to surveillance measures at any time without notification pursuant to the Special Surveillance Means Act (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2007, §§ 69-94); the interception and recording of a conversation by means of a radio-transmission device in the framework of a secret police operation without any procedural safeguards (*Bykov v. Russia* [GC], 2009, §§ 72-83); the recording of conversations in the framework of an "operative experiment" conducted at the initiative of the Federal Security Service in a manner not "in accordance with the law" (*Oleynik v. Russia*, 2016, §§ 74-79); the warranted interception by the Defence Ministry of outgoing communications by organisations working in the civil liberties field (*Liberty and Others v. the United Kingdom*, 2008, §§ 55-70); the storage of records on and police surveillance of an applicant on account of his membership of a human rights organisation (*Shimovolos v. Russia*, 2011, §§ 64-71); secret surveillance legislation setting up a special anti-terrorist task force without adequate safeguards against abuse (*Szabó and Vissy v. Hungary*, 2016, §§ 52-89); storage of

information collected by means of secret surveillance (*Rotaru v. Romania* [GC], 2000, §§ 45-63; *Association « 21 December 1989 » and Others v. Romania*, 2011, §§ 169-177); various deficiencies in the domestic legal framework governing secret surveillance of mobile phone communications (*Roman Zakharov v. Russia* [GC], 2015, §§ 163-305); and a regime of bulk interception of communications which did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse, even though certain robust safeguards were identified (*Centrum för rättvisa v. Sweden* [GC], 2021, §§ 365-374, and *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 424-427). The Court also found a violation of Article 8 in *Ekimdzhiev and Others v. Bulgaria*, 2022 (§§ 356-359 and 419-421), observing, in particular, that although significantly improved after they were examined in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2007, the laws governing secret surveillance, as applied in practice, still fell short of the minimum safeguards against arbitrariness and abuse in a number of aspects. A similar finding was reached as regards laws governing the retention of communications data and its subsequent accessing by the authorities.

147. The Court found no violation of Article 8 in the following cases: the use of an undercover agent in tandem with tapping the telephone line of the applicant, who had been charged with drug-trafficking (*Lüdi v. Switzerland*, 1992, §§ 38-41); a system authorising secret surveillance of the general public's correspondence, mail and telephone communications (*Klass and Others v. Germany*, 1978, §§ 39-60); and a legislative framework authorising interception of domestic communications in order to combat terrorism and serious crime (*Kennedy v. the United Kingdom*, 2010, §§ 151-170).

148. The Court declared manifestly ill-founded the case of *Weber and Saravia v. Germany* (dec.), 2006 (§§ 143-153) concerning strategic surveillance of telecommunications, a follow-up case to *Klass and Others v. Germany*, 1978.

b. Data collection by employers in the workplace

149. The Court has assessed under Article 8 the issue of personal data collection at the workplace by public-sector employers (*Halford v. the United Kingdom*, 1997, §§ 49, 45; *Antović and Mirković v. Montenegro*, 2017, § 58; *Libert v. France*, 2018, § 41) or private (*Köpke v. Germany* (dec.), 2010; *Bărbulescu v. Romania* [GC], 2017, § 109; and *López Ribalda and Others v. Spain* [GC], 2019, § 109). In some cases the data collection operation had been carried out without the data subjects' knowledge, by means of surveillance which was kept secret, either totally (*Halford v. the United Kingdom*, 1997, § 49; *Copland v. the United Kingdom*, 2007, § 45; *Bărbulescu v. Romania* [GC], 2017, § 78), or partly (*López Ribalda and Others v. Spain* [GC], 2019, § 93), while in other cases the data had been collected with the full knowledge of the employees concerned (*Antović and Mirković v. Montenegro*, 2017, § 44).

150. The personal data to be collected originated in: surveillance of non-professional phone calls from professional premises (*Halford v. the United Kingdom*, 1997, § 44); monitoring of telephone, e-mail and Internet usage at work (*Copland v. the United Kingdom*, 2007, §§ 44-49); monitoring of Internet and instant messaging (Yahoo) usage (*Bărbulescu v. Romania* [GC], 2017, § 74); opening of files stored by an employee on a computer provided by his employer for work purposes (*Libert v. France*, 2018, § 25); pictures taken via a video recording showing the conduct of an identified or identifiable employee at his workplace (*Köpke v. Germany* (dec.), 2010; *Antović and Mirković v. Montenegro*, 2017, § 44; *López Ribalda and Others v. Spain* [GC], 2019, § 92); or monitoring, by means of a GPS system, of the distances travelled by an employee in a company vehicle in the course of his professional activity and, as applicable, on private journeys (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, §§ 94-96).

151. In the first two judgments delivered in this sphere (*Halford v. the United Kingdom*, 1997, § 44, and *Copland v. the United Kingdom*, 2007, § 41), the Court held that non-professional telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence"

for the purposes of Article 8. It also considered that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage (*Copland v. the United Kingdom*, 2007, § 41). Subsequently, the Court also specified that data clearly identified as private and stored by an employee in a computer provided to him by his employer for work purposes might also be covered by the "private life" concept (*Libert v. France*, 2018, § 25). Furthermore, a covert video recording showing the conduct of an employee at his workplace, without notification, also affects his "private life" (*Köpke v. Germany* (dec.), 2010). Subsequently, the Court discerned no reason to depart from this conclusion whether the video surveillance of employees at their workplace was secret or overt (*Antović and Mirković v. Montenegro*, 2017, § 44; *López Ribalda and Others v. Spain* [GC], 2019, § 93).

152. In the cases of *Halford v. the United Kingdom*, 1997 (§§ 50-51) and *Copland v. the United Kingdom,* 2007 (§ 48), the Court found that in the absence, at the material time, of a domestic legal provision authorising the collection of personal data from non-professional telephone calls by employees and from electronic messages sent from the workplace, respectively, the resultant interference with their right to respect for private life had not been "in accordance with the law". In the case of *Köpke v. Germany* (dec.), 2010, the Court declared manifestly ill-founded a complaint about an employer who had collected data on a supermarket cashier suspected of theft, with the help of a private detective agency, using covert video surveillance. Even though at the material time the conditions under which an employer could resort to video surveillance of an employee had not yet been laid down in legislation, the case-law of the Federal Labour Court had set out major safeguards against arbitrary interference in employees' right to respect for their private life.

153. The existence of reasonable suspicion that serious misconduct has been committed and the extent of the losses identified in the present case may constitute weighty justification for employers to implement personal data-collection in the workplace (*López Ribalda and Others v. Spain* [GC], 2019, § 134). Conversely, mere suspicions of misappropriation or any other wrongdoing on the part of employees cannot justify the installation of covert video-surveillance by the employer (ibid., § 134).

154. In *Bărbulescu v. Romania* [GC], 2017 (§ 121) the Court defined a number of criteria to be met in respect of measures geared to supervising employees' correspondence and communications at their workplace if they were not to fall foul of Article 8. In that context, the national authorities have to answer the following questions: was the employee notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures? What was the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy? Did the employer provide legitimate reasons to justify monitoring the employee's communications? Would it have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications? What were the consequences of the monitoring for the employee subjected to it? Had the employee been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature? And finally, the domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful (ibid., § 122).

155. Subsequently, in *López Ribalda and Others v. Spain* [GC], 2019 (§ 116), the Court pointed out that those criteria were transposable to video-surveillance measures implemented by an employer in the workplace. In *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 (§ 115), the Court further applied the said criteria in the context of monitoring *via* a GPS system by an employer of the distances travelled by an employee in a company vehicle.

156. The Court has found violations of Article 8 in cases where it has noted a failure on the part of the domestic courts to ensure that an employer's implementation of surveillance measures was proportionate and accompanied by adequate and sufficient safeguards. In the case of *Bărbulescu*

v. Romania [GC], 2017 (§§ 108-141), the national courts had failed to determine the specific reasons justifying the implementation of surveillance measures, whether the employee could have resorted to less intrusive measures *vis-à-vis* the employee's private life and correspondence, or whether the employee had been notified in advance by his employer of the possible monitoring of his communications. Conversely, in *Libert v. France*, 2018 (§§ 37-53) the Court found no violation of Article 8 regarding the opening of personal files stored in a work computer, the pornographic content of which had provided the grounds for the employee's dismissal. It observed that domestic law as interpreted and applied by the domestic court, had comprised adequate safeguards against arbitrariness, including the fact that the employer had only been allowed to open the files marked "personal" in the employee's presence.

157. In the Court's view, only an overriding requirement relating to the protection of significant public or private interests could justify a failure on the employer's part to provide employees with prior information on measures liable to infringe the protection of employees' personal data (*López Ribalda and Others v. Spain* [GC], 2019, § 133). Before implementing measures to collect their data, employers should inform the employees concerned of the existence and conditions of such data collection, even if only in a general manner (ibid., § 131). The transparency requirement and the consequent right to information are fundamental, particularly in the context of employment relationships, where the employer has significant powers with regard to employees, and any abuse of those powers should be avoided. However, the provision of information to the individual being monitored and its extent constitute just one of the criteria to be taken into account in order to assess the proportionality of a measure of this kind in a given case. However, if such information is lacking, the safeguards deriving from the other criteria will be all the more important (ibid., § 131).

158. Where no prior information has been provided, it is important to ascertain whether the employees who had been subjected to surveillance had had domestic remedies at their disposal specifically intended to ensure effective protection of the right to respect for private life. In the framework of measures imposed on employees at the workplace, such protection may be ensured by various means, which may fall within employment law but also civil, administrative or criminal law (ibid., § 136).

159. With more specific regard to video surveillance of employees, in *López Ribalda and Others v. Spain* [GC], 2019 (§ 125) the Court has pointed out that it is necessary to distinguish, in the analysis of the proportionality of a video-surveillance measure, the various places in which the monitoring was carried out, in the light of the protection of privacy that an employee could reasonably expect. That expectation is very high in places which are private by nature, such as toilets or cloakrooms, where heightened protection, or even a complete ban on video-surveillance, is justified (ibid., §§ 125, 61, 65, citing the relevant international instruments). It remains high in closed working areas such as offices, and is manifestly lower in places that are visible or accessible to colleagues or to the general public (ibid., § 125).

160. In that connection, in the case of *Köpke v. Germany* (dec.), 2010, the Court declared inadmissible as manifestly ill-founded the complaint raised by the applicant, a supermarket cashier, concerning a covert video-surveillance measure implemented by her employer with the help of a private detective agency. The Court observed in particular that the impugned measure had been limited in time (two weeks) and had only covered the area accessible to the public around the cash desk, that the video data obtained had been processed by a limited number of persons working for the detective agency and the employer's staff, and that they had been used solely in the framework of the applicant's dismissal procedure and the proceedings before the labour courts.

161. Conversely, in the judgment in the case of *Antović and Mirković v. Montenegro*, 2017 (§§ 55-60), the Court found a violation of Article 8 on the grounds that the alleged infringement of the private life of the applicants, two university professors, as a result of the installation of a video-surveillance system in the university auditoriums where they held classes, was not prescribed by law.

162. In *López Ribalda and Others v. Spain* [GC], 2019 (§ 137), the Court found no violation of Article 8 in respect of partly overt and party covert video-surveillance of cashiers and sales assistants in a supermarket, having regard, *inter alia,* to the substantial safeguards provided by Spanish legislation, including remedies of which the applicants had not availed themselves.

163. Likewise, *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022 (§§ 105-125) concerned the applicant's dismissal on the basis of mileage data recorded by means of a GPS system installed on his company vehicle by his employer. The Court found no violation of Article 8, having considered that the domestic courts had carefully balanced the competing interests at stake namely, the applicant's right to respect for his private life and his employer's right to ensure the smooth running of the company, taking into account the legitimate aim pursued by the company, namely the right to monitor its expenditure.

c. Data collection for use in evidence in court cases

164. The collection of real evidence in the framework of court cases raises issues linked to the protection of individuals' personal data, whatever their status in the proceedings in question, as parties, witnesses or third parties.

i. Searches and seizures

165. In several cases the Court has emphasised that the Contracting States might have considered it necessary to have recourse to measures such as searches and seizures in order to obtain physical evidence of certain offences (*Vasylchuk v. Ukraine*, 2013, § 79; *K.S. and M.S. v. Germany*, 2016, § 43). In such cases, scrutiny of the measures will target the relevance and adequacy of the reasons given to justify them, as well as compliance with the principle of their proportionality to the aim pursued (*Smirnov v. Russia*, 2007, § 44). The seriousness of the offence which prompted the search and seizure, the circumstances in which the order was issued, in particular whether any further evidence was available at that time, the content and scope of the order, having particular regard to the nature of the premises searched and the safeguards implemented in order to confine the impact of the measure to reasonable bounds, the manner in which the search was conducted and the extent of possible repercussions on respect for the private life of the person concerned, are all important criteria to be taken into account in balancing the various competing interests (ibid., § 44; *Modestou v. Greece*, 2017, § 42 and the references therein). The Court also requires domestic law to provide adequate and sufficient safeguards against arbitrariness (*Vinci Construction and GTM Génie Civil and Services v. France*, 2015, § 66; *Modestou v. Greece*, 2017, § 43). Such guarantees include the existence of "effective scrutiny" of measures encroaching on Article 8 (ibid., § 42).

166. In the case of *Trabajo Rueda v. Spain*, 2017 (§§ 44-47), the seizure of the applicant's personal computer, which had enabled the police to access all the personal files stored in the computer on the grounds that it contended child pornographic materials, was deemed contrary to Article 8. The Court had not been convinced of the urgency of the situation requiring the police to seize the files from the applicant's personal computer and to access all the data stored without obtaining the prior judicial authorisation normally required, even though such authorisation could have been obtained fairly quickly.

167. In *K.S. and M.S. v. Germany*, 2016 (§§ 32-58), the Court found no violation of Article 8 as regards a search of the applicants' home under a warrant issued on the basis of information comprising personal data unlawfully copied by a bank employee and then sold to the secret services, concerning their assets in a bank abroad. German legislation and practice provided adequate and effective guarantees against abuse. Furthermore, the domestic courts had not overstepped their margin of appreciation in basing the search warrant on data originating abroad. In particular, the Court attached particular weight to the fact that at the time the search warrant had been issued, few, if any, relevant data sets other than the one at issue had been purchased by German authorities (ibid., § 51). Nor does

the fact alone that there is no absolute rule that evidence which has been acquired in violation of the procedural rules cannot be used in criminal proceedings, imply that the authorities deliberately obtained the data in breach of international or domestic law (ibid., § 51). Moreover, the data carrier contained information concerning the financial situation of the applicants, which they were obliged to submit to the domestic tax authorities, but no data closely linked to their identity (ibid., § 53; compare *G.S.B. v. Switzerland*, 2015, § 93, concerning the transmission of bank details to the tax authorities in another State under a bilateral agreement).

168. Searches conducted in business premises aimed at collecting real evidence raise issues as regards protecting their data, from the angle of the right to respect for their "correspondence" and "home" as secured under Article 8. For example, in the case of *Bernh Larsen Holding AS and Others v. Norway*, 2013 (§§ 104-175) the Court found no violation of Article 8 as regards a decision ordering a company to provide a back-up copy of all the data in the computer server which it shared with other companies. While no requirement of prior judicial authorisation applied, the Court took account of the effective and adequate safeguards against abuse, the interests both of the companies and their employees, and the public interest in effective tax inspection (ibid., §§ 172-175). Conversely, the Court noted a violation of Article 8 in *DELTA PEKÁRNY a.s. v. Czech Republic*, 2014 (§§ 92-93), concerning an inspection of business premises aimed at securing evidence of the existence of an illegal agreement on prices in breach of the rules on competition. The Court referred to the lack of prior authorisation by a judge, of effective *post hoc* review of the necessity of the measure and of regulations on the possible destruction of the data obtained.

169. In the case of *Buck v. Germany*, 2005 (§§ 30-53), the search of the applicant's business and residential premises in connection with a road traffic offence committed by a third person had amounted to a violation of Article 8. Having regard to the special circumstances of this case, in particular the fact that the search and seizure in question had been ordered in connection with a minor contravention of a regulation purportedly committed by a third person and comprised the private residential premises of the applicant, the Court concluded that the interference could not be deemed proportionate to the legitimate aims pursued (ibid., § 52).

170. Concerning searches of journalists' professional premises, homes and private vehicles (in some cases), and mass seizures, for the purposes of identifying their sources, the Court found a violation of Article 8 in the case of *Ernst and Others v. Belgium*, 2003 (§§ 110-117). In connection with action to combat breaches of the secrecy of judicial investigations, the Contracting States' legislation and practice, which can provide for home searches and seizures, must provide adequate and sufficient guarantees against abuse. That had not been the situation in the present case since no charges had been brought against the applicants and the various search warrants had been broadly worded, providing no information on the impugned investigation, the specific premises to be searched or the items to be seized, thus leaving the investigators with extensive room for manoeuvre. Furthermore, the applicants had never been informed of the actual reasons for the searches (see also paragraph 328 below concerning the violation of Article 10 in this case).

171. As regards seizures carried out in legal practices, they must always be accompanied by special procedural safeguards such as to protect the data confidentiality which underpins the relationship of trust between lawyer and client[8]. In the case of *Kırdök and Others v. Turkey*, 2019 (§§ 52-58), the seizure of several lawyers' electronic data by the judicial authorities for the purposes of criminal proceedings against another lawyer who shared those lawyers' office, and the refusal to return the data or to destroy them had amounted to a breach of Article 8. The Court attached weight to the fact that no procedure had been noted during the search for filtering electronic documents or data covered by professional secrecy. Further, the refusal to return the seized data on the grounds that since they

[8] See also Guide on Article 8 of the Convention (right to respect for private and famili lifle) *f*or further details on the procedure guarantees applicable to seizures carried out in legal practices.

had not yet been transcribed there was no way of ascertaining to whom they belonged, was not clearly prescribed by law and was contrary to the very essence of professional secrecy, which called for the confidentiality of those data.

172. In *Kruglov and Others v. Russia*, 2020 (§§ 123-138), the Court ruled that seizures of computers and hard drives containing personal information and documents covered by the professional secrecy of the applicants, who were lawyers by profession, or of their clients, during searches conducted by the police in their homes and offices, without any filtering of the data seized, had been contrary to Article 8. In particular, the existence of prior judicial authorisation has a limited effect because the domestic courts had never attempted to balance the obligation to protect data confidentiality against the needs of the criminal investigation, for example by considering the possibility of obtaining information from other sources (ibid. , §§ 126-129).

173. The Court also found a violation of Article 8 in the case of *Smirnov v. Russia*, 2007 (§§ 36-49), concerning a search and seizure of a large number of documents and the central unit of a lawyer's computer, in the lawyer's home, without justification or guarantee; in the case of *Wieser and Bicos Beteiligungen GmbH v. Austria*, 2007 (§§ 42-68), concerning searches and the seizure of a lawyer's electronic data in breach of the procedural safeguards provided for by law; in *Robathin v. Austria*, 2012 (§ 52), relating to an insufficiently reasoned authorisation for the search and seizure of all the electronic data stored in a legal practice; and in the case of *Särgava v. Estonia*, 2021 (§§ 107-108), concerning procedural safeguards that were considered insufficient to protect the data covered by professional secrecy after the seizure and then the examination of a lawyer's computer and mobile phone.

174. In the case of *Vinci Construction and GTM Génie Civil and Services v. France*, 2015 (§§ 69-81), the Court found a violation of Article 8 in respect of a search and seizure of computer data belonging to companies, including e-messages covered by the confidentiality of lawyer-client relations. The trial court, while acknowledging the presence of correspondence from a lawyer among the documents seized by the investigators, had merely assessed the lawfulness of the formal framework for the impugned seizures without conducting the requisite detailed examination.

175. In *André and Others v. France*, 2008 (§§ 37-49), a "home" search and seizure of documents in a legal practice by tax officers with a view to obtaining evidence against one of its client companies had amounted to a violation of Article 8. The purpose of the search at issue had been to discover at the premises of the applicants, purely in their capacity as the lawyers of the company suspected of fraud, documents capable of establishing the existence of such fraud on the company's part and to use such documents in evidence against it. At no stage had the applicants been accused or suspected of having committed an offence or been involved in fraud committed by their client company (ibid., § 46).

176. A second seizure effected five minutes after the return of unlawfully confiscated material had amounted to a violation of Article 8 in the case of *Visy v. Slovakia*, 2018 (§§ 33-47). The applicant had been deprived of any effective guarantees against arbitrariness and abuse as regards the second seizure.

177. In *Sher and Others v. the United Kingdom*, 2015 (§§ 171-176), a terrorism case, the Court had to examine the question of a search warrant which was extendable in cases of suspected terrorist activities. The Court held that the complexity inherent in such cases could justify a search based on terms that are wider than would otherwise be permissible. To impose under Article 8 the requirement that a search warrant identify in detail the precise nature of the items sought and to be seized could seriously jeopardise the effectiveness of an investigation where numerous lives might be at stake. In cases of this nature, the police must be permitted some flexibility to assess, on the basis of what is encountered during the search, which items might be linked to terrorist activities and to seize them for further examination (ibid., § 74).

178. In *Ivashchenko v. Russia*, 2018 (§§ 59-95), the customs authorities' powers to consult and copy individuals' electronic data amounted to a violation of Article 8, in the absence of reasonable suspicions of wrongdoing. The copying of the applicant's personal and professional data, followed by its communication for a specialist assessment, and the retention of his data for some two years, had exceeded what could be considered as unintrusive "routine" procedures for which consent was usually given. The applicant had been unable to choose whether he wanted to present himself and his belongings to customs and a possible customs inspection. (See also *Gillan and Quinton v. the United Kingdom,* 2010, §§ 61-67, concerning powers to stop and search individuals without any plausible reasons for suspecting them of having committed an offence, amounted to a violation of Article 8. The Court pointed out that the public nature of the search, during which embarrassment was caused by the fact of having personal information exposed to other people, could even, in certain cases, compound the seriousness of the interference in the individual's private life because of the element of humiliation and embarrassment. The discretion enjoyed by police officers was a source of concern: not only was it unnecessary for them to demonstrate the existence of any reasonable suspicion, but they were not required even subjectively to suspect anything about the person stopped and searched).

ii. Compulsory medical acts for the purposes of cellular sampling

179. Broadly speaking, the use of various compulsory medical acts for the purposes of cellular sampling, such as blood tests and buccal swabs, was no prohibited as such in the context of taking evidence in civil or criminal proceedings (*Caruana v. Malta* (dec.), 2018, § 41).

180. In the case of *Mikulić v. Croatia*, 2002 (§ 64), the Court considered that the lack of any procedural measure to compel the alleged father to submit to DNA testing was only in conformity with the principle of proportionality if it provided alternative means of determining the paternity claim. The Court found a violation of Article 8 because there were no such means under domestic law, thus condemning the applicant to further prolonged uncertainty as to her personal identity owing to her presumed father's refusal to submit to DNA testing (ibid., §§ 65-66).

181. In *Mifsud v. Malta*, 2019 (§§ 61-78), a court order issued to the applicant to undergo genetic testing against his will, in paternity proceedings, pursuant to Maltase law, had not been contrary to Article 8. Before ordering the applicant to submit to DNA testing the domestic courts had conducted the requisite balancing exercise with regard to the competing interests in the case, in the framework of judicial proceedings in which the applicant had taken part, represented by counsel of his choosing, and in which his procedural rights had been respected on an equal footing with the opposing party. The domestic courts had thus struck a fair balance between the interest of the applicant's presumed daughter to have paternity established and that of the applicant not to undergo the DNA tests (ibid., § 77). All in all, the decision-making process had been fair and had properly protected the applicant's interests as secured under Article 8.

182. In the case of *Boljević v. Serbia*, 2020 (§§ 50-56), the Court ruled that the dismissal by the domestic courts as statute-barred of an application for review of a final decision given forty-one years previously allowing a man's action contesting paternity, at a time when DNA testing had not yet existed, had been contrary to Article 8. The Court took the view that the preservation of legal certainty could not suffice in itself as grounds for depriving the applicant of the right to know the truth about an important aspect of his personal identity, without balancing the competing interests in the case. Domestic law on time-limits for reopening proceedings had prevented the authorities from conducting such a balancing exercise, having regard to the very specific circumstances of the applicant's case, namely that the applicant had only learnt of the final judgment concerning his purported father's paternity following the latter's death. The Court held that the private life of a deceased person from whom a DNA sample is to be taken cannot be adversely affected by a request to that effect made after his death. The Court had previously reached the same decision in *Succession Kresten Filtenborg Mortensen v. Denmark* (dec.), 2006, concerning the exhumation of a corpse for genetic testing, and

Jäggi v. Switzerland, 2006 (§ 42), where a refusal by the courts to authorise DNA testing on a deceased person as requested by the latter's alleged son in order to ascertain the identity of his natural father had amounted to a violation of Article 8 (ibid., §§ 34-44).

183. In *Caruana v. Malta* (dec.), 2018 (§§ 28-42), the Court declared manifestly ill-founded a complaint relating to the obligation imposed on the wife of a presumed murderer to give buccal samples. The Court held that a buccal swab was a minor intervention which seldom caused bodily injury or physical or mental suffering. Murder was a serious criminal offence, and so it was both reasonable and necessary to gather as much evidence as possible (ibid., § 41). Furthermore, the Court drew a distinction between the situation of a witness and that of an accused, whose refusal to undergo such a measure in the context of criminal proceedings, which could have a bearing on an eventual finding of guilt and related sanctions (ibid., § 40).

184. In the case of *Dragan Petrović v. Serbia*, 2020 (§§ 79-84), a buccal swab in the framework of a murder inquiry amounted to a violation of Article 8 owing to the lack of foreseeable legal provisions. The fact that the applicant had agreed to give a sample of his saliva to the police officers was of no relevance to whether or not he had sustained interference in his private life, because he had done so only under the threat that either a saliva sample or a blood sample would otherwise be taken from him by force (ibid., § 79).

185. The Court also found a violation of Article 8 in the case of medical data collection from Jehovah's Witnesses who had refused blood transfusions (*Avilkina and Others v. Russia*, 2013); see also paragraph 188 above.

186. Violations of Article 8 were also found in a case of organ removal from the bodies of deceased persons for the purposes of transplantation without the knowledge or consent of the deceased's close relatives (*Petrova v. Latvia*, 2014, §§ 87-98), and in a situation of imprecision of the domestic legislation on consent from close relative to the removal of tissue from the body of a deceased person (*Elberte v. Latvia*, 2015, §§ 105-117).

d. Personal data collection in a medical context

187. The Court has dealt with the matter of collecting sensitive data in the medical sphere. In the case of *L.H. v. Latvia*, 2014 (§§ 47-60), the collection of medical data on a patient in a public hospital by a State agency ("the agency") responsible for controlling the quality of health care was found not to comply with Article 8, in the absence of precisely formulated legislation affording adequate legal protection against arbitrariness. The agency had collected the data in question over a seven-year period, indiscriminately, without any prior assessment of whether the data collected would be "potentially decisive", "relevant" or "of importance" in pursuit of the aim of the investigation. The agency had not been required to request and obtain the applicant's consent to the collection of his data (ibid., § 53). The scope of private data that could be collected was not limited in any way (ibid., § 57). Moreover, the relevance and sufficiency of the reasons for collecting the information appeared not to have been examined at any stage of the domestic procedure (ibid., § 57). In this context, the Court considered that it was less relevant whether the agency had a legal duty to maintain the confidentiality of personal data (ibid., § 58).

188. In the case of *Surikov v. Ukraine*, 2017 (§§ 75-95), the collection and retention of personal data concerning a person's mental health for an extended period, as well as the communication and use of that data for purpose unconnected with the initial reasons for their collection had amounted to a disproportionate interference with the data subject's right to respect for his private life, in breach of Article 8. Although employers could have a legitimate interest in information concerning their employees' mental and physical health, particularly in the context of assigning them certain job functions connected to specific skills, responsibilities or competences, the collection and processing of the relevant information had to be lawful and such as to strike a fair balance between the

employer's interests and the privacy-related concerns of the candidate for the relevant position (ibid., § 91).

189. In *Z v. Finland*, 1997 (§§ 106-110), the Court found no violation of Article 8 concerning a seizure of medical files and their inclusion in the investigation file without the prior consent of the patient, in the framework of criminal proceedings against her husband. There had been no irregularities in the decision-making process, and remedies had been available to challenge the seizure and to annul the time-limit set out in the confidentiality order.

190. The case of *Drelon v. France*, 2022 (§§ 79-100) concerned the applicant's attempt to donate blood at a collection site of the French Blood Donation Service and their refusal to accept him as a blood donor based on his presumed homosexuality. Even though the applicant had refused to answer the questions about his sex life during the pre-donation medical interview, the data included a contraindication to giving blood that was specific to men who had intercourse with other men. Having noted the sensitive nature of the said data, the Court accepted that their collection and storage were based on relevant and sufficient reasons, notably the protection of health and the importance of ensuring blood safety. At the same time, it noted that the data collected were based on mere speculation without any proven factual basis. It also noted the excessive length of the data retention which made it possible for the data to be used repeatedly against the applicant, resulting in his automatic exclusion from donating blood. With reference to those elements, the Court found a violation of Article 8 of the Convention.

e. Compulsory communication of personal data

191. The Court has on a number of occasions assessed the obligation on mobile phone operators, Internet service providers, banks, elite athletes, and hospitals to provide to the authorities personal data in their possession under a law or an order issued by the authorities.

192. As regards action against organised crime and terrorism, the Court has accepted that investigative methods have to be tailored to modern communications technology. In the case of *Breyer v. Germany*, 2020 (§§ 81-110), the legal obligation on mobile phone operators to record the personal data of prepaid SIM card users and to make them available to the authorities, pursuant to the Telecommunications Act, which authorised various public authorities to request the retrieval and communication of such data without any need for a judicial decision or notification of the persons concerned, was not deemed contrary to Article 8. Only a limited data set was stored, and no data concerning individual communication events was stored; the interference had therefore been fairly minor (ibid., §§ 92-95). There had also been a number of safeguards: technical security insurance, limited storage period, data confined to requisite information for clearly identifying the subscriber in question; regulated facilities for future consultation and use of the stored data; supervision by an independent authority; and appeal facilities for anyone considering that his rights had been breached, although the level of review and supervision was not a decisive element in the proportionality assessment of the collection and storage of such a limited data set (ibid. , §§ 96-107).

193. Conversely, the Court has considered that the imposition of a legal obligation on Internet service providers to retrieve the stored connection data or one of their subscribers and to transmit it to the police amounted to a violation of Article 8 because the legal provisions relied upon by the police had been unclear and had provided no protection against arbitrary interference, particularly in the absence of independent supervision of the police powers in issue (*Benedik v. Slovenia*, 2018, §§ 132-134).

194. In the case of *Sommer v. Germany*, 2017 (§ 63), the inspection of a lawyer's bank account had amounted to a violation of Article 8 in view of the low threshold for inspecting the applicant's bank account, the wide scope of the requests for information, the subsequent disclosure and continuing storage of the applicant's personal information, and the insufficiency of procedural safeguards.

195. In the case of *Avilkina and Others v. Russia*, 2013 (§ 54), regarding the collection of medical data on Jehovah's Witnesses who had refused blood transfusions, the Court held that the collection by the prosecution of data on the applicants from the medical institution which had treated them, without informing the data subjects or giving them an opportunity to object, had been incompatible with Article 8. The prosecutor's office had had other options in following up the complaints submitted to it against the religious organisation in question, such as questioning the individuals in question or seeking their consent (ibid., § 48).

196. In *National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, 2018 (§§ 155-191), the legal requirement as to whereabouts imposed on a "testing pool" of elite athletes, for the purposes of carrying out unannounced doping tests as part of an anti-doping drive, entailing heavy penalties from the third failure to comply within a period of eighteen consecutive months, was not deemed contrary to Article 8. Without underestimating the impact of the whereabouts requirements on the applicants' private lives, the Court considered that reducing or removing the requirements imposed on elite athletes would be liable to increase the dangers of doping to their health and to that of the entire sporting community, and would run counter to the European and international consensus on the need for unannounced testing (ibid. , § 191).

197. In the case of *Aycaguer v. France*, 2017 (§§ 45-47), the Court found a violation of Article 8 on the grounds that the applicant's criminal conviction for refusing to undergo a compulsory biological test for the purposes of recording his DNA profile in the national computerised database of convicted persons, could not be regarded as a measure which was necessary in a democratic society. the applicant had carried out the actions which had led to the order to undergo a compulsory DNA test in a political/trade-union context, concerning mere blows with an umbrella directed at gendarmes who had not even been identified, for which he had been sentenced to two months' imprisonment, suspended. However, no differentiation was provided for in the national computerised DNA database according to the nature and seriousness of the offence committed, notwithstanding the significant disparity in the situations potentially arising, as witness the applicant's situation (ibid., § 43). Finally, the applicant had not had access to any procedure for the deletion of stored data (such a procedure was provided solely for persons suspected of an offence, and not for persons already convicted) (ibid., § 43).

2. Retention of personal data

198. The storing by a public authority of information relating to an individual's private life, however that information is obtained, amounts to an interference with the right to respect for the data subject's private life within the meaning of Article 8, whether or not the data is subsequently used (*Amman v. Switzerland* [GC], 2000, § 69; *Rotaru v. Romania* [GC], 2000, § 46; *S. and Marper v. the United Kingdom* [GC], 2008, § 67; *M.K. v. France,* 2013, § 29; *Aycaguer v. France,* 2017 § 33). The intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned (*S. and Marper v. the United Kingdom* [GC], 2008, § 104).

a. Storage of personal data for the purposes of combating crime

199. The interests of data subjects and the community as a whole in protecting personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (*S. and Marper v. the United Kingdom* [GC], 2008, § 104). In order to protect their population as required, the national authorities can legitimately set up databases as an effective means of helping to punish and prevent certain offences, including the most serious types of crime, such as sex offences (*B.B. v. France*, 2009, § 62; *Gardel v. France*, 2009, § 63; *M.B. v. France,* 2009, § 54). While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting

in the identification of future offenders (*S. and Marper v. the United Kingdom* [GC], 2008, § 100). The Court cannot call into question the preventive purpose of such registers (*Gardel v. France*, 2009, § 63; *B.B. v. France*, 2009, § 62; *M.B. v. France,* 2009, § 54). The fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification (*S. and Marper v. the United Kingdom* [GC], 2008, § 105). At the same time, since 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, domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (ibid. , § 103).

200. The Court has considered a series of cases relating to the recording in databases designed for the punishment and prevention of crime the personal data of individuals convicted of minor offences (*M.K. v. France*, 2013, §§ 6, 8, 41; *Aycaguer v. France*, 2017, §§ 8, 43), serious offences (*B.B. v. France*, 2009, §§ 6, 62; *Gardel v. France*, 2009, §§ 8, 9, 63; *M.B. v. France,* 2009, §§ 6, 54; *Peruzzo and Martens v. Germany* (dec.), 2013, §§ 6, 12, 37-38; *Trajkovski and Chipovski v. North Macedonia*, 2020, §§ 6, 12), or for a series of offences that were neither minor nor particularly serious (*P.N. v. Germany*, 2020, §§ 6, 81). Other cases concerned the storage, in databases designed for the punishment and prevention of crime, of the personal data of individuals who had been suspected of committing offences but who had ultimately been discharged (*S. and Marper v. the United Kingdom* [GC], 2007, §§ 10, 11, 113; *M.K. v. France*, 2013, §§ 7, 9, 42; *Brunet v. France*, 2014, §§ 6, 7, 40), acquitted (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 10, 113), or simply cautioned after the proceedings, without conviction (*M.M. v. the United Kingdom*, 2012, §§ 7-9). Lastly, other cases have concerned preventive measures involving storing personal data in police files, on the basis of mere suspicions (*Shimovolos v. Russia*, 2011, § 16; *Khelili v. Switzerland*, 2011, §§ 8, 9, 59; *Catt v. the United Kingdom*, 2019, §§ 6, 14, 119).

201. The factors set out below are important in considering the necessity of storing personal data for police purposes.

i. Indiscriminate and undifferentiated nature of data stored

202. In several cases the Court has called into question the broad scope of the data storage system installed by the authorities, which failed to draw a distinction according to the nature or degree of seriousness of the offence leading to conviction (*M.K. v. France*, 2013, § 41; *Aycaguer v. France,* 2017, § 43; *Gaughran v. the United Kingdom*, 2020, § 94), or depending on whether the data subject had been convicted, acquitted, discharged or merely cautioned, having been suspected of committing an offence (*S. and Marper v. the United Kingdom* [GC], 2008, § 119; *M.M. v. the United Kingdom*, 2012, § 198; *M.K. v. France*, 2013, § 42*; Brunet v. France*, 2014, § 41). The Court considers that the facilities put in place by the authorities to assist in punishing and preventing certain offences cannot be implemented as part of an abusive drive to maximise the information stored in them. Indeed, without respect for the requisite proportionality *vis-à-vis* the legitimate aims assigned to such mechanisms, their advantages would be outweighed by the serious breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction (*M.K. v. France,* 2013, § 35 ; *Aycaguer v. France,* 2017, § 34).

203. In *S. and Marper v. the United Kingdom* [GC], 2008 (§§ 119, 125), a database in which it was possible to collect and store fingerprints, biological samples and DNA profiles from anyone suspected but not convicted of criminal offences, whatever their age, the nature and seriousness of the offences, without a time-limit or any independent review of the justification of the retention of data according to defined criteria, had led to a finding of a violation of Article 8. The blanket and indiscriminate nature of such a system failed to reflect a fair balance between the competing public and private interests.

204. There is a risk of stigmatisation where persons who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons (*S. and Marper v. the United Kingdom* [GC], 2008, § 122). Even though the retention of private data concerning individuals suspected of an offence but acquitted or discharged cannot be equated with the voicing of suspicions, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed (ibid., § 122). Therefore, the fact that a person has benefited from a discharge after being suspected of an offence justifies treating him differently from a convicted person (ibid., § 122; see also, to the same effect, *M.K. v. France*, 2013, § 42; *Brunet v. France*, 2014, § 40). Thus in *Brunet v. France*, 2014 (§ 40), where the applicant had benefited from a discontinuance decision following mediation, the Court called into question the indiscriminate nature of the personal data recorded in the authorities' files, drawing no distinction between convicted persons and individuals whose cases had been discontinued. In the case of *Aycaguer v. France,* 2017 (§§ 42-43), where personal data had been collected and retained following a conviction for offences which were not the most serious, the Court called into question the broad scope of the personal data collection by the authorities, which had drawn no distinction according to the level of seriousness of the offence leading to conviction, notwithstanding the wide range of situations liable to arise in the framework of the application of the law. In the Court's view, the acts leading to the applicant's conviction, mere blows with an umbrella directed at gendarmes in a political/trade-union context, had not been comparable to acts that were classified as particularly serious offences, such as sex offences, terrorism, crimes against humanity or human trafficking.

205. In the case of *M.M. v. the United Kingdom*, 2012 (§§ 187-207), the lifelong entry of a caution in the police records of a person after she had gone missing for a day with her grandson, a baby, hoping to prevent his departure for Australia following the breakdown of her son's marriage, had led to a finding of a violation of Article 8. The Court called into question the extremely extensive scope of the data retention system, which covered not only convictions but also non-conviction decisions such as warnings, cautions and reprimands, as well as a large amount of supplementary data recorded by the police by virtue of a general guideline to the effect that data should be retained until the data subject had reached the age of 100 (ibid., § 202). The Court considered that the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data (ibid., § 200). The same applied to the case of *Gaughran v. the United Kingdom,* 2020 (§§ 94-97), concerning the indefinite storage of the biometric data and photographs of the applicant, who had been convicted of driving with excess alcohol, amounting to a violation of Article 8.

206. The retention of unconvicted persons' data may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society. particular attention should be paid to the protection of juveniles from any detriment of that type (*S. and Marper v. the United Kingdom* [GC], 2008, § 124).

ii. Data retention period

207. The length of the period for which the authorities decide to store an individual's personal data is an important, albeit not a decisive, aspect to be taken into account in assessing whether or not the storage of personal data in a file or a database for police purposes is proportionate to the legitimate aim pursued. The Court found violations of Article 8 in cases concerning:

- indefinite storage of fingerprints of and DNA data on persons who were suspected of an offence but whose proceedings had ended with a discontinuance decision or an acquittal (*S. and Marper v. the United Kingdom* [GC], 2008);

- indefinite storage of the DNA profiles, fingerprints and photographs of an individual found guilty of an offence, even after his conviction had been deleted from his police record on expiry of the legal time-limit (*Gaughran v. the United Kingdom*, 2020);
- lifelong retention on a police record of all the convictions, acquittals, cautions, warnings and reprimands pertaining to one individual (*M.M. v. the United Kingdom*, 2012);
- indefinite storage of the DNA profiles of persons convicted of aggravated theft (*Trajkovski and Chipovski v. Macédoine du Nord*, 2020);
- retention for a maximum forty years of the personal data of an individual convicted of a fairly minor offence (*Ayçaguer v. France*, 2017);
- retention for a maximum twenty years of the fingerprints of an individual suspected, but not convicted, of stealing books (*M. K. v. France*, 2013);
- retention for a maximum twenty years of the personal data of an individual following a complaint of violence against his partner, which case was discontinued following mediation (*Brunet v. France*, 2014);
- retention until 2278 of personal data on the applicant's presumed homosexuality collected in 2004 (*Drelon v. France*, 2022).

208. Conversely, the Court found no violation of Article 8 in several cases concerning the storage of the personal data of individuals convicted of sexual assault for a maximum thirty years, after which period the data was automatically deleted, because procedures had been introduced to enable the data to be deleted as soon as it was no longer relevant (*B.B. v. France*, 2009, § 67; *Gardel v. France*, 2009, § 69; *M.B. v. France,* 2009, § 59). The Court also declared manifestly ill-founded a case concerning the indefinite retention of the personal data of persons convicted of serious offences, accompanied by reviews at regular intervals of no longer than ten years, to determine whether the data storage was still necessary (*Peruzzo and Martens v. Germany* (dec.), 2013, §§ 44-49). In the case of *P.N. v. Germany*, 2020 (§§ 87-90), the Court found no violation of Article 8 with regard to the retention for five years, subject to guarantees and individualised review, of a repeat offender's personal data for the purposes of identifying him following the commencement of fresh criminal proceedings against him.

209. In respect of retention regimes for the biometric data of convicted persons, the duration of the retention period is not necessarily conclusive in assessing whether a State has overstepped the acceptable margin of appreciation in establishing the relevant regime - the existence and functioning of certain safeguards is decisive (*Gaughran v. the United Kingdom*, 2020, § 88). When States themselves set retention limits for the biometric data of convicted persons, or indeed decide that data retention should be indefinite, they are putting themselves at the limit of their margin of appreciation and must ensure the existence of certain effective safeguards (ibid., § 88). The existence or lack of independent review of the justification for retention of the information according to defined criteria such as the seriousness of the offence, the strength of the suspicion against the person, previous convictions and any other special circumstances, is a major safeguard for ensuring the proportionality of data retention periods (ibid., § 94; *S. and Marper v. the United Kingdom* [GC], 2008, § 119; *B.B. v. France*, 2009, § 68; *Gardel v. France*, 2009, § 69; *M.B. v. France,* 2009, § 60).

210. The lack of a maximum period for the retention of personal data is not necessarily incompatible with Article 8 (*Peruzzo and Martens v. Germany* (dec.), 2013, § 46; *Gaughran v. the United Kingdom*, 2020, § 88), but procedural safeguards are especially necessary where the storing of the data depends entirely on the diligence with which the authorities ensure the proportionality of the data retention period (*Peruzzo and Martens v. Germany* (dec.), 2013, § 46; *Ayçaguer v. France*, 2017, § 38).

211. In *Peruzzo and Martens v. Germany* (dec.), 2013 (§ 44) concerning the indefinite retention of the biometric data of persons convicted of serious offences liable to recidivism, the Court was satisfied to note that domestic law required the Federal Criminal Office to check at regular intervals of no more

than 10 years, whether the data storage was still necessary or if the data could be deleted, having regard in each case to the purpose of the data retention and the nature and gravity of the circumstances of each case in which personal data was recorded (ibid., § 46). The Court held that the length of the intervals had not been unreasonable given that the DNA profiles could only be obtained from persons convicted of offences reaching a specific threshold of gravity (ibid. , §§ 48-49).

212. In the case of *Gaughran v. the United Kingdom*, 2020 (§ 96), the indefinite nature of the storage of the fingerprints, DNA profiles and photograph of an individual found guilty of driving with excess alcohol had led to a finding of a violation of Article 8. The authorities had not had regard to the seriousness of the offence committed or to the continuing need to retain the said data indefinitely, nor had they provided any real review facilities (ibid., § 96).

213. A maximum storage period for personal data laid down in domestic law may be more akin, in practice, to a norm than to a real maximum if the chances of acceptance of a request for deletion of the data before expiry of the period laid down by law are merely hypothetical (*M. K. v. France*, 2013, §§ 44-47; *Brunet v. France*, 2014, §§ 41-45; *Ayçaguer v. France*, 2017, §§ 44-46). The Court has found a violation of Article 8 in several cases where the national system provided for maximum periods of storage of twenty or twenty-five years for offences in which proceedings had been discontinued (*M. K. v. France*, 2013, §§ 44-47; *Brunet v. France*, 2014, §§ 41-45), and indeed a maximum forty-year storage period in the case of an offence that had not been particularly serious but which had led to a conviction (*Ayçaguer v. France*, 2017, § 42).

214. In *Catt v. the United Kingdom*, 2019 (§ 120), the retention of the applicant's personal data in a national police database on extremism for at least six years, after which period it would be subject to a scheduled review had led to a finding of a violation of Article 8. The applicant had been completely dependent on the authorities' diligence in implementing the highly flexible safeguards laid down in the applicable code of practice, in ensuring the proportionality of the data retention period. The lack of safeguards to facilitate the deletion of the data as soon as the period of retention became disproportionate is particularly disturbing where data revealing political opinions, which attracts a heightened level of protection, is being retained indefinitely (ibid., §§ 122-123).

215. The case of *M.M. v. the United Kingdom*, 2012 concerned the consequences of changes of policy on the retention period for personal data on a criminal record in terms of the data subject's employment prospects (§ 204). The Court considers that the indiscriminate and open-ended collection of criminal record data is unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, *inter alia*, the duration of the storage of such data (ibid., § 199).

216. See also, in a different context, the ten-year limit set by a court on the confidentiality of evidence produced during proceedings containing medical data such as to reveal the identity and HIV-positive status of an individual in the case of *Z v. Finland*, 1997 (§§ 111-113). In this case the ten-year confidentiality period was at variance with the wishes and the interests of the parties to proceedings, and the production, without the applicant's consent, of the information in question had already occasioned a serious interference with her right to respect for her private and family life. The further interference which she would suffer if the medical information were to be made accessible to the public after ten years was not supported by any compelling reasons.

iii. Safeguards concerning the destruction or deletion of data stored[9]

217. In the Court's view, the deletion of data from a database in which it had been stored for police purposes was not particularly burdensome (*Catt v. the United Kingdom*, 2019, § 127). It would be entirely contrary to the need to protect private life under Article 8 if the Government could create a

[9] See also the section above on the Right to data deletion ("right to be forgotten").

database in such a manner that the data in it could not be easily reviewed or edited, and then use this development as a justification to refuse to remove information from that database (ibid., § 127).

218. The availability at the national level of a judicial procedure for the removal of data that provides for independent review of the justification for retention of the information according to defined criteria and affords adequate and effective safeguards of the right to respect for the data subject's private life is an important factor in balancing the various competing interests (*S. and Marper v. the United Kingdom* [GC], 2008, § 119; *Gardel v. France*, 2009, § 69).

219. The Court has found no violation of Article 8 in cases where, even though the data had been retained for "long" periods of up to thirty years (*B.B. v. France*, 2009, §§ 66, 68; *Gardel v. France*, 2009, §§ 67, 69; *M.B. v. France,* 2009, §§ 58, 60), or indeed indefinitely (*Peruzzo and Martens v. Germany* (dec.), 2013, § 46), the data subject had benefited from a judicial procedure guaranteeing independent review of the justification for storing their data according to defined criteria, enabling them to secure the deletion of the data before expiry of the maximum period prescribed by law, or, in the case of indefinite data retention, as soon as such retention was no longer relevant (see, to converse effect, *S. and Marper v. the United Kingdom* [GC], 2008, § 119).

220. Thus in *B.B. v. France*, 2009 (§ 68), *Gardel v. France*, 2009 (§ 69), and *M.B. v. France,* 2009 (§ 60), the Court ruled that the judicial procedure for the removal of data, which the data subject could initiate on simple request to the public prosecutor, whose decisions were subject to judicial appeal, provided for independent review of the justification of retaining the information according to defined criteria and afforded adequate and effective safeguards. See also paragraph 204 above, concerning the case of *Peruzzo and Martens v. Germany* (dec.), 2013 (§ 44).

221. In the case of *P.N. v. Germany*, 2020 (§§ 81, 88) concerning the storage of the personal data of an adult offender whose offences had been neither minor nor particularly serious, the rule to the effect that such data was deleted after a five-year period in the absence of any new criminal investigations regarding the data subject within that period, was not deemed contrary to Article 8. There was a possibility of review by the police authorities, subject to judicial review, of the necessity of further retaining the data in question, and the applicant could thus secure the removal of his data if his conduct showed that the data was no longer required for police purposes (ibid., § 88).

222. The absence of effective safeguards permitting the deletion of personal data which are no longer relevant for the initial purposes is of particular concern as regards sensitive categories of personal data attracting a heightened level of protection (*Catt v. the United Kingdom*, 2019, § 123).

223. The possibility under domestic law of deleting data is a "theoretical and illusory" guarantee rather than a "practical and effective" safeguard where the right to submit at any time a request for such deletion is liable to clash with the interests of the investigative services in having a file with the largest possible number of references and where the competing interests at stake are contradictory, if only partially (*M.K. v. France,* 2013, § 44). The safeguard on deletion of data is also of limited impact where the authorities refuse, following a request from the data subject to delete his data or to provide any explanation for its continued retention (*Catt v. the United Kingdom*, 2019, § 122). The same is true where deletion requests are only allowed under exceptional circumstances, or are rejected where the data subject admitted having committed an offence and the data are accurate (*M.M. v. the United Kingdom*, 2012, § 202).

224. The Court takes the view that individuals who have been convicted of an offence should, like persons who have been acquitted or discharged, also be given a practical means of lodging a request for the deletion of registered data (*B.B. v. France*, 2009, § 68; *Brunet v. France*, 2014, §§ 41-43; *Ayçaguer v. France*, 2017, § 44). In *Ayçaguer v. France*, 2017 (§ 44), where a data deletion procedure was only available for persons suspected of having committed an offence and not for convicted persons, the Court found a violation of Article 8. The Court considered that owing to its duration and

the lack of any possibility of deletion, the regulations on the storing of DNA profiles in the national database did not strike a fair balance between the competing public and private interests (ibid., § 45).

225. In the case of *Khelili v. Switzerland*, 2011 (§§ 68-70) the Court found a violation of Article 8, highlighting the uncertainties and difficulties which the applicant had encountered in her attempts to secure the deletion of the "prostitute" entry in the "occupation" section of the police file, since she had never been convicted of having unlawfully prostituted herself. The Court noted that it had never been claimed that the deletion of the impugned entry in the police file had been impossible or difficult for technical reasons (ibid., § 68).

iv. Guarantees aimed at regulating access by third parties and protecting data integrity and confidentiality

226. The Court has on several occasions considered whether or not the applicable domestic law comprised guarantees capable of efficiently protecting personal data stored in official databases from misuse and abuse (*S. and Marper v. the United Kingdom* [GC], 2008, § 103; *B.B. v. France*, 2009, § 61; *Gardel v. France*, 2009 § 62; *M.M. v. the United Kingdom*, 2012, § 195; *M.K. v. France,* 2013, § 35; *Brunet v. France*, 2014, § 35; *Ayçaguer v. France*, 2017, § 38). It noted that such guarantees were in place where, for example,

- only authorities bound by a duty of confidentiality could consult registered data (*B.B. v. France*, 2009, § 69; *Peruzzo and Martens v. Germany* (dec.), 2013, § 47);
- the registered data was subject to sufficiently well-defined procedures as regards consultation, concerning the persons authorised to consult the database (*M.K. v. France,* 2013, § 37; see, to converse effect, *Khelili v. Switzerland*, 2011, § 64);
- the identity of a person from whom a DNA sample had been taken had not been disclosed to the experts responsible for DNA profiling; the latter had also been required to adopt appropriate measures to prevent any unauthorised use of the cellular material examined (*Peruzzo and Martens v. Germany* (dec.), 2013, § 45); the cellular material itself had to be immediately destroyed once it was no longer needed for the purpose of establishing the DNA profile, and only DNA profiles extracted from such cellular material could be retained in the Federal Criminal Police Office's database (ibid., § 45); moreover, the DNA profiles retained could only be disclosed to the relevant authorities for the purposes of criminal proceedings, the preventive aversion of dangers and for international legal assistance in respect thereof (ibid., § 47).

227. In *Gardel v. France*, 2009 (§ 70), where the rules on the use of the register and the range of public authorities with access to it had been extended on several occasions and were no longer limited to the judicial authorities and the police, administrative bodies now also having access, the Court was satisfied to note that the register could only be consulted by authorities that were bound by a duty of confidentiality, and in precisely defined circumstances.

228. In the case of *P.N. v. Germany*, 2020 (§ 89), there was nothing to indicate that the identification data taken from an adult offender and stored by the police for a maximum five years were insufficiently protected against abuse such as unauthorised access or dissemination.

229. Conversely, in *M.M. v. the United Kingdom*, 2012 (§ 204), concerning the lifelong retention of a caution on an individual's police record and the disclosure of that data to a future employer in a job-seeking context, the Court called into question the failings in the procedure governing third-party access to the criminal records of job-seekers, which did not allow for assessment at any stage of the relevance of the data held in central records to the employment sought, or of the extent to which the data subject could be perceived as continuing to pose a risk.

b. Retention of medical data

230. The Court has dealt with the issue of the storage of sensitive health-related data. In the case of *Malanicheva v. Russia* (dec.), 2016 (§§ 13, 15-18), the Court held that the efficient functioning of healthcare institutions and the judicial decision-making process necessitated the storage and sharing of relevant data. It rejected as manifestly ill-founded the complaints concerning the registration of the applicant's name on the hospital register of persons suffering from psychiatric disorders and allegedly erroneous references to various aspects of her mental health in the subsequent internal communications between the healthcare institutions and in their observations before the courts. Nothing indicated that the registered information in question had been made accessible to the public or been used for any other purpose than deciding on the most suitable medical care for the data subject.

231. Previously, the Commission had declared manifestly ill-founded and rejected a case concerning the recording in a psychiatric hospital file of data on the compulsory confinement of a patient, which had been declared unlawful by the domestic courts (*Yvonne Chave née Jullien v. France*, 1991). The Commission held that the recording of information concerning mental patients serves 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, since it helped prevent the risk of arbitrary confinement, and was a means of investigation at the disposal of the administrative or judicial authorities responsible for the oversight of psychiatric institutions. In this case the applicant's personal data recorded on the psychiatric hospital register had been protected by appropriate confidentiality rules.

232. See also paragraph 182 above concerning the violation of Article 8 in the case of *Surikov v. Ukraine*, 2017 (§ 75-95).

c. Online storage of personal data for journalistic purposes

233. In *M.L. and W.W. v. Germany*, 2018 (§ 90), the Court stated that the press had a secondary but nonetheless valuable role in maintaining archives containing news which had previously been reported and making them available to the public. In that regard, Internet archives make a substantial contribution to preserving and making available news and information, since they constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free (*Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, 2009, §§ 27, 45; *Węgrzynowski and Smolczewski v. Poland*, 2013, § 59).

3. Disclosure of personal data

234. In several cases the Court has assessed measures entailing the disclosure of an individual's personal data by the data processor, to:

- another individual or a legal person (*Mockutė v. Lithuania*, 2018, §§ 99-100, concerning the transmission by a hospital of information on a patient's state of health to a member of her family and to journalists; *Y. v. Turkey* (dec.), 2015, §§ 70-72, concerning the disclosure by an ambulance crew to hospital staff of information on a patient's HIV-positive status; *Radu v. Republic of Moldova*, 2014, § 27, concerning the disclosure by a hospital of medical information on a patient to her employer; *M.C. v. the United Kingdom*, 2021, § 46 concerning the disclosure by the authorities of information concerning the applicant's criminal record to her prospective employer);
- a public authority (*M.S. v. Sweden*, 1997, § 35, concerning the disclosure by a gynaecological department of medical information on a patient to a social security fund; *P.T. v. Republic of Moldova*, 2020, §§ 5-6, 29-31, concerning the unnecessary inclusion of sensitive medical data on a certificate to be produced in various contexts);

- the public (*Hájovský v. Slovakia*, 2021 §§ 46-49, on the publication in a television news broadcast of information identifying an individual and containing a non-blurred photo of him taken covertly and under false pretence; *Peck v. the United Kingdom*, 2003, § 63, on the transmission to the media of a closed-circuit TV video showing a person attempting to commit suicide in a public place; *Bremner v. Turkey*, 2015, §§ 71-85, concerning the TV broadcast of an unblurred, unpixellated image of an individual filmed by a hidden camera; *Khadija Ismayilova v. Azerbaijan*, 2019, §§ 108-132, concerning a covert video recording of a journalist in her private home and the public broadcasting of the videos; *Z v. Finland*, 1997, §§ 70-71, concerning the disclosure in a judicial decision transmitted to the press of an individual's identity and state of health; *Apostu v. Romania*, 2015, §§ 121-132, on the disclosure to the press of pieces of evidence from an investigation file; *Montera v. Italy* (dec.), 2002, concerning the public disclosure of a report by a parliamentary commission on a magistrate's private life and professional ethics; *Von Hannover v. Germany*, 2004, §§ 61-81, on the publication in the tabloid press of photographs relating to a princess's private life; *Polanco Torres and Movilla Polanco v. Spain*, 2010, §§ 44-54, concerning a press article based on statements by a former accountant accusing a senior judge's wife of involvement in unlawful transactions with a specified company; *Alkaya v. Turkey*, 2012, §§ 30-31, concerning the disclosure by a mass-circulation daily newspaper of a famous actress's full postal address; *Mityanin and Leonov v. Russia*, 2018, §§ 111-121, on the dissemination in the press of a photograph of a suspect, accompanied by statements accusing him of various minor and serious criminal offences; and *Bogomolova v. Russia*, 2017, §§ 54-58, concerning the publication of a photograph of a child on the cover page of a booklet entitled "Children need a family", published by a Centre for Psychological, Medical and Social Support).

a. Impact of prior consent

235. Prior consent by data subjects to the transmission, disclosure or publication of their data is an important, although not a decisive, element in determining in a given case whether such operations amount to interference with their right to respect for private life (*M.S. v. Sweden*, 1997, §§ 31, 35; *M.M. v. the United Kingdom*, 2012, §§ 186, 189) or if they can be considered as being "in accordance with the law" within the meaning of Article 8 § 2 (*Radu v. the Republic of Moldova*, 2014, § 27; *Mockutė v. Lithuania*, 2018, § 101). The Court found a violation of Article 8 in several cases in which the disclosure of personal data by the data processor had occurred without the consent of the data subject (*Radu v. the Republic of Moldova*, 2014, §§ 30, 32; *Mockutė v. Lithuania*, 2018, §§ 103, 106; *Peck v. the United Kingdom*, 2003, §§ 85-87; *Sõro v. Estonia*, 2015, §§ 17-19, 64).

236. In order to be valid, the data subject's consent must be informed and unequivocal (*M.S. v. Sweden*, 1997, § 32; *Konovalova v. Russia*, 2014, §§ 47-48). In a case concerning the communication of an individual's medical file by one public body (a hospital gynaecological department) to another (the Social Security Department) without the data subject's consent, the issue was whether, by bringing an action for damages, the data subject had waived her right to data confidentiality (*M.S. v. Sweden*, 1997, §§ 31-32). The Court ruled that since the data disclosure had depended not only on fact that applicant had submitted a compensation claim but also on a number of factors beyond her control, it could not be inferred from her request for compensation that she had unequivocally waived her right to respect for private life with regard to the medical records. Accordingly, Article 8 had applied.

237. The fact that individuals' personal data are disclosed at their request or with their consent does not deprive them of the protection afforded by Article 8 if they have no real choice, for example if an employer insists on disclosure of personal data stored on a job-seeker's criminal record (*M.M. v. the United Kingdom*, 2012, § 189). In the latter case *M.M. v. the United Kingdom*, 2012 (§§ 187-207), where the applicant had requested the disclosure to a potential employer of information on a caution registered in her criminal record, the Court found a violation of Article 8 owing to the lack of sufficient

safeguards in the system for retention and disclosure of criminal record data, which had not provided for an assessment at any stage of the allowed relevance of the data to the employment sought, or of the extent to which the data subject could be perceived as continuing to pose a risk (ibid., § 204). In *M.C. v. the United Kingdom*, 2021, §§ 47-57, the Court noted the legislative changes introduced following *M.M. v. the United Kingdom* and found that a newly introduced regime for disclosure of information about a criminal record was compatible with the relevant requirements of Article 8: it distinguished between different types of offences in different ways; provided certainty as to what previous convictions would be disclosed at any given time; and established a defined, finite period of time for disclosure which would vary depending on the age of the offender and the perceived seriousness of the offence.

238. Obtaining the data subject's consent is not always feasible, for example where footage from closed-circuit cameras installed in the street by the authorities in order to help identify offenders and prevent crime includes images of numerous persons (*Peck v. the United Kingdom*, 2003, § 81). In the Court's view, a closed-circuit TV camera system, the disclosure of images from which is based on consent, could in practice undermine any action aimed to promote the effectiveness of the CCTV system in detecting and preventing criminal offenses, which role is rendered even more effective through advertising the CCTV system and its benefits (ibid., § 81). In those circumstances, or where individuals included in CCTV footage refuse to consent to the dissemination of their images, the data processor should consider other solutions, such as masking the images before dissemination (ibid., § 82) or ensuring that the receivers of the images mask them themselves, in an appropriate and adequate manner (ibid., § 83).

239. In *Peck v. the United Kingdom*, 2003 (§ 87), the communication by a borough council in a press release for the media of images from a closed-circuit TV filming an individual attempting to commit suicide in a public place had amounted to a violation of Article 8. The Court held that since the footage in question clearly focused on and related to one individual only, the CCTV operator who had alerted the police and observed their intervention could have made enquiries with the police to establish the identity of the applicant and thereby request his consent to disclosure (ibid., § 81).

240. In the case of *Bremner v. Turkey*, 2015 (§§ 71-85), the broadcasting, in a television documentary filmed by a hidden camera, of an unblurred, unpixellated image of an individual was deemed contrary to Article 8. As regards, in particular, the fact that the applicant was not well known, there was nothing to suggest that the said transmission had any inherent informative value or had been properly and adequately used.

241. Furthermore, having regard to the chilling effect to which a pre-notification requirement risks giving rise, to the significant doubts as to the effectiveness of any pre-notification requirement and to the wide margin of appreciation enjoyed by the national authorities in this area, the Court found, in *Mosley v. the United Kingdom*, 2011 (§ 132), that Article 8 did not call for a legally binding requirement on notifying a person before publishing information on his private life.

242. In some situations the disclosure of data on an individual's mental health without his or her consent to a close relative can amount to a violation of the right to respect for his or her private life. In the case of *Mockutė v. Lithuania*, 2018 (§ 100), the Court found that the disclosure to a patient's mother of information on the health of her adult daughter without the latter's consent, in view of the tense relationship between the two adult individuals, had been incompatible with the right secured under Article 8.

243. As regards persons under arrest or prosecution, the Court found violations of Article 8 where police services had handed over photographs of the applicants to the press without their consent (*Sciacca v. Italy*, 2005, §§ 29-31; *Khuzhin and Others v. Russia*, 2008, §§ 115-118), where they had invited TV crews to film an applicant at a police station without his consent with a view to broadcasting the images on television (*Toma v. Romania*, 2009, §§ 90-93; *Khmel v. Russia*, 2013, § 41), or in a case

where posting up a photograph of the applicant on the "wanted" noticeboard had not been prescribed by law (*Guiorgui Nikolaïchvili v. Georgia*, 2009, §§ 129-131).

244. Failure to obtain the data subject's prior consent to the transmission, disclosure or publication of his data does not necessarily amount to a violation of Article 8 if there are other legitimate concerns such as the necessity of investigating criminal offences and ensuring the publicity of judicial proceedings (*Avilkina and Others v. Russia,* 2013, § 45; *Z v. Finland*, 1997, § 97), and the need to protect public health (*Y. v. Turkey* (dec.), 2015, § 74), national security (*Anchev v. Bulgaria* (dec.), 2017, § 100) or a country's economic well-being (*M.S. v. Sweden*, 1997, § 38).

b. Disclosure of data in the context of judicial proceedings

245. In several cases the Court has examined measures adopted by the authorities in the context of judicial proceedings having led to the disclosure of the parties' or third parties' personal data, such as:

- the reproduction by a court in a divorce judgment of an extract from personal medical records (*L.L. v. France*, 2006, § 46), and an order restricting to ten years the period of confidentiality of evidence produced containing medical data (*Z v. Finland*, 1997, §§ 112-113);
- the disclosure of confidential psychiatric data on an applicant during a public hearing (*Panteleyenko v. Ukraine*, 2006, § 57), and verification of a medical certificate produced in support of a request for adjournment (*Stokłosa v. Poland* (dec.) 2021, §§ 43-44;
- the disclosure of an individual's identity and HIV-positive status in a judgment communicated to the press (*Z v. Finland*, 1997, § 113);
- the disclosure of the full identity of a third party in a judgment without prior notification of the latter (*Vicent Del Campo v. Spain*, 2018, §§ 47-51);
- the use of language and arguments disclosing, in a judgment, personal data of the victim, conveying stereotypes about the role of women and capable of hindering the effective protection of the victims of sexual violence in spite of a satisfactory legislative framework (*J.L. v. Italy*, 2021, §§ 136-142).

246. In the Court's opinion, the necessity of protecting the confidentiality of certain types of personal data may sometimes be outweighed by the interest in the investigation and prosecution of crime and in the publicity of court proceedings (*Avilkina and Others v. Russia,* 2013, § 45; *Z v. Finland*, 1997, § 97). The competent national authorities should be afforded some leeway in striking a fair balance between, on the hand, the protection of the publicity of judicial proceedings, which is necessary to uphold trust in the courts, and on the other hand, the interests of a part or of a third person in maintaining the confidentiality of his data (*C.C. v. Spain*, 2009, § 35). Any measure liable to make public an individual's personal data, whether he is a party or a third party to judicial proceedings, should meet an overriding social need (*Vicent Del Campo v. Spain*, 2018, § 46) and should be limited as far as possible to that which is rendered strictly necessary by the specific features of the proceedings (*L.L. v. France*, 2006, § 45).

247. In order to determine, in any given case, whether there are sufficient grounds for disclosing, in the body of a judicial decision, the identity of an individual and other personal data on the latter, one important question is whether other less intrusive measures would have been possible under domestic law and practice. This includes of the possibility of a court omitting mentioning any names in the judgment permitting the identification of the data subject (*Z v. Finland*, 1997, § 113; *Vicent Del Campo v. Spain*, 2018, § 50), keeping the full reasoning confidential for a certain period and instead publishing an abridged version of the reasoning, the operative part and an indication of the law which it had applied (*Z v. Finland*, 1997, § 113), or restricting access to the text of a judgment or to certain matters therein (*Vicent Del Campo v. Spain*, 2018, § 50). The Court considers that such measures are

generally deemed capable of reducing the impact of a judgment on the data subject's right to protection of his private life.

248. In the case of *Panteleyenko v. Ukraine,* 2006 (§ 82), the Court held that a private hearing might also have helped prevent the public disclosure during a public hearing of confidential information on an individual's mental health obtained from a psychiatric hospital and on his psychiatric treatment there, although it would not necessarily have prevented that information from being brought to the attention of the parties and being included in the case-file.

249. In *Frâncu v. Romania*, 2020 (§§ 72-73), the failure of a court of appeal to ensure the confidentiality of medical information on the applicant by dismissing a request for a private hearing in a corruption case against a mayor was deemed contrary to Article 8. In the Court's view, by merely declaring, without further explanations, that the applicant's case did not correspond to "any of the situations" set out in the Code of Criminal Procedure concerning proceedings held in private session, that court had failed to strike a fair balance between the general interest in ensuring the transparency of judicial proceedings and the litigant's interest in preserving the confidentiality of the data on his state of health. Even supposing that an accused person' high public profile may be one of the factors to be taken into account in analysing the proportionality of a request for a private hearing, in this case the court of appeal conducted no individualised assessment of the proportionality of such a measure.

250. In the case of *Khadija Ismayilova v. Azerbaijan*, 2019 (§§ 105-132), the Court ruled that the disclosure by the prosecuting authorities of private information including sensitive personal data such as the name and address of the applicant, a professional journalist, as well as her friends', relatives' and colleagues' names in a press release purportedly setting out a progress report on a criminal investigation, had amounted to a violation of Article 8 (ibid., §§ 142-150).

251. In the case of *M.P. v. Portugal*, 2021, §§ 48-49, the production by the applicant's ex-husband, without her consent, in the context of divorce proceedings, of electronic messages exchanged by his wife on a dating site to which she seemed to have given him access did not entail a violation of Article 8, as the Family Court had not ultimately taken them into account and public access to data in this type of procedure was, in any event, restricted.

252. In *J.S. v. the United Kingdom* (dec.), 2015 (§§ 71-73), the Court rejected as manifestly ill-founded a complaint concerning the disclosure in a press release from the Public Prosecution Service of personal information which had not gone beyond that routinely provided to the media in response to queries about court proceedings and had not disclosed the applicant's name, age or school (he was a minor accused of assaulting a teacher), nor any other personal information.

253. In the case of *L.L. v. France*, 2006 (§§ 46), in which the judge had relied, on an alternative and secondary basis, in the framework of divorce proceedings, on private correspondence between a medical consultant and the applicant's general practitioner containing a confidential medical document, the fact that the judge or the investigating officer could have excluded the medical data in question from the reasoning of the judgment and still have arrived at the same conclusion was an important factor that should be taken into account. Since anyone could have obtained a copy of the reasoning of the decision without having to prove a particular interest, the interference sustained by the applicant in his right to respect for his private life had not been justified in view of the fundamental role played by personal data protection, notwithstanding that proceedings between parties to a divorce were not public and the decision which was valid *vis-à-vis* third parties contained only the operative provisions (ibid., §§ 47, 33).

254. In the case of *Vicent Del Campo v. Spain*, 2018 (§§ 53, 56), the fact that the applicant, a third party to judicial proceedings, had been deprived of any opportunity for asking a court, before delivery of the judgment, to refrain from communicating his identity had amounted to a violation of Article 8. The applicant had not been informed, questioned, summoned to appear or notified in any manner whatever.

255. In a case in which the domestic courts had limited to ten years the period for the confidentiality of documents in the case-file disclosing the applicant's identity and HIV-positive status, the Court found a violation of Article 8 on the grounds that the judicial authorities had attached insufficient weight to the interests of protecting the parties' and third parties' personal data liable to be affected (*Z v. Finland*, 1997, §§ 111-112). It considered that the serious interference with her right to respect for her private life occasioned by the production in judicial proceedings, without her consent, of information concerning her state of health, would be further aggravated if the medical information in question were to be made accessible to the public after ten years (ibid., § 112). Conversely, in *Y. v. Turkey* (dec.), 2015 (§§ 81-82), the fact that the applicant's identity and HIV-positive status had been disclosed in a single decision to decline jurisdiction given by an administrative court, which had not been published or made public in any other way, and was not accessible to the public, while none of the other decisions given in the context of the same proceedings had referred to it, had not been deemed liable to infringe the data subject's right to respect for her private life.

256. In the case of *Drakšas v. Lithuania*, 2012 (§ 60), the disclosure in the context of impeachment proceedings of recordings of telephone conversations intercepted by the secret services between the applicant, a well-known politician, and the President who was being impeached, at a public hearing before the Constitutional Court broadcast live on the national television channels, had not amounted to a violation of Article 8. The Court took the view that as a public figure the applicant had inevitably and knowingly laid himself open to close scrutiny of his every word and deed by both journalists and the public at large. That being the case, the disclosure, prescribed by law, of his non-private political or commercial telephone conversations during constitutional proceedings had been necessary for the protection of the rights of others.

257. See also paragraph 243 above concerning disclosure to the press by police services of photographs of persons under arrest or prosecution without their consent, and paragraphs 80 to 82 above in connection with the positive obligations on the State in cases concerning the disclosure of personal data by private individuals.

c. Disclosure of data for the protection of public health

258. A person's right to respect for medical secrecy is not absolute and must be considered in relation to other legitimate rights and interests, such as his or her employer's right to adversarial proceedings (*Eternit v. France* (dec.), 2012, § 37). That right may be outweighed by the need to protect a fundamental aspect of the public interest, such as the safety of hospital staff and the protection of public health (*Y. v. Turkey* (dec.), 2015, § 74).

259. In cases of treatment of patients within the hospital and health system, transmission of information on the patient's condition may, under certain circumstances, be relevant and necessary for the purposes of not only guaranteeing appropriate medical treatment for the patient but also ensuring the protection of the rights and interests of the healthcare providers involved in his treatment and of other patients, by enabling the requisite precautionary measures to be adopted (*Y. v. Turkey* (dec.), 2015, § 74). Where medical workers themselves run a risk of infection owing to their exposure in the course of their duties, hospital staff security and the protection of public health can justify the transmission of information on a patient's state of health among the medical personnel involved in his or her treatment in order to prevent any risk of in-hospital transmission of the disease (ibid., § 78).

260. Sensitive information such as data on a patient's state of health should be transmitted in such a way as to prevent any form of stigmatisation of the data subject and to provide sufficient safeguards to eliminate any risk of abuse (*Y. v. Turkey* (dec.), 2015, § 79). The receiver of the information should be subject to the specific rules on confidentiality relevant to health professionals or similar confidentiality requirements (ibid., § 74).

261. In *Y. v. Turkey* (dec.), 2015 (§§ 78-79), the Court rejected as manifestly ill-founded an application concerning the exchange of information on a patient's HIV-positive status among the various healthcare providers in a hospital where he had undergone treatment, on the grounds that such information-sharing had been justified by the security of the hospital staff and the protection of public health, notwithstanding the fact that the data subject had not given his consent. The Court attached importance to the fact that under domestic law all healthcare providers had been required to respect the confidentiality of any data transmitted to them in the context of their situation or occupation, on pain of disciplinary or criminal sanctions.

d. Disclosure of data for the protection of national security

262. In a series of cases concerning the dismantling of the heritage of the former communist regimes, the Court has considered the issue of the public disclosure of data relating to the distant past of an individual as collected and stored for the purposes of protecting national security (*Sõro v. Estonia*, 2015, § 58; *Anchev v. Bulgaria* (dec.), 2017, § 100). Importance is attached to the individualised measures implemented for the dismantling process, their regulation and the safeguards provided.

263. Thus, in *Sõro v. Estonia*, 2015 (§§ 56-64), the disclosure of information to the effect that the applicant had been employed as a chauffeur in the former security services had amounted to a violation of Article 8. Even though the applicant had been informed in advance that the data was to be published and had been able to challenge the data communication, there had been no procedure in place to assess the specific tasks performed by individual employees of the former security services in order to differentiate the danger they could possibly pose in a democratic system several years after the termination of their career in these institutions (ibid., § 61). The Court held that any threat the applicant could initially have posed to the newly created democracy must have considerably decreased with the passage of time between the restoration of independence in Estonia and the publication of the personal data (ibid., § 62). Even though the Disclosure Act had not *per se* imposed any restrictions on the applicant's new employment, he had been forced to resign from his position owing to the attitude adopted by his colleagues, which was indicative of the seriousness of the interference with the applicant's right to respect for his private life (ibid., § 63).

264. Conversely, in the case of *Anchev v. Bulgaria* (dec.), 2017 (§§ 92-116), in which the disclosure procedure had been strictly regulated and been accompanied by a number of safeguards against arbitrariness and abuse, including the fact that it had been entrusted to a special independent commission whose decisions were subject to judicial review at two levels of jurisdiction, public disclosure of data relating to the applicant's distant past had been deemed incompatible with Article 8. Since the disclosure had not entailed any sanctions or legal disabilities, the interference had not exceeded the substantial margin of appreciation enjoyed by the authorities (ibid., §§ 106-113). The Court stated that its conclusion might have been different if the State had implemented measures involving more serious intrusion into the data subject's personal sphere, such as a prohibition on working or partial deprivation of voting rights (ibid., § 113).

e. Disclosure of data for the protection of the economic well-being of the country

265. Measures which are supposed to ensure the protection of the country's economic well-being and which infringe the confidentiality of data collected or stored by the authorities are not necessarily contrary to Article 8 if they are accompanied by effective and satisfactory safeguards (*M.S. v. Sweden*, 1997, § 41). In balancing the various competing interests, the questions whether domestic law regulates the measures liable to be adopted by the data processors, whether their responsibility is engaged in the event of non-compliance with legal requirements, and whether the receiver of the data has an obligation to observe similar rules and guarantees and in particular a duty of confidentiality, are important aspects which must be taken into account (ibid., § 43).

266. In *M.S. v. Sweden*, 1997 (§§ 31-44), the transmission of an individual's medical records by one public body (a hospital gynaecological department) to another (the Social Security Department), responsible for assessing whether the applicant satisfied the legal conditions for entitlement to a benefit which she had herself applied for, had not been in breach of Article 8. The Court held that that data communication had potentially been decisive for the allocation of public funds to deserving claimants and could thus be regarded as having pursued the aim of protecting the economic well-being of the country (ibid., § 38). The disclosure of the applicant's confidential data had been accompanied by effective and satisfactory safeguards against abuse: under the relevant domestic legislation it was a condition for imparting the data concerned that the information had to be of importance for the application of the occupational disability insurance act (ibid., §§ 18, 43); the civil and/or criminal liability of members of the gynaecological department staff could have been engaged if they had failed to comply with those conditions (ibid., §§ 22, 43); and the receiver of the data had had a similar duty to respect their confidentiality (ibid., §§ 20, 22, 43).

f. Mass disclosure of personal data

267. The existence of a public interest in providing access to, and allowing the collection of, large amounts of taxation data did not necessarily or automatically mean that there was also a public interest in disseminating *en masse* such raw data in unaltered form without any analytical input. In the case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 (§ 175), the Court emphasised that a distinction should be drawn between the processing of data for journalistic purposes and the dissemination of the raw data to which the journalists were given privileged access. The fact of preventing the bulk disclosure of personal taxation data, under procedures incompatible with national regulations and the EU rules on data protection, is not in itself a sanction, even if the limitations imposed on the quantity of the information to be published may, in practice, have rendered some of the applicant companies' business activities less profitable (ibid., § 197).

B. Data subjects' rights

268. The Court's case-law grants personal data subjects a number of specific rights to guarantee their enjoyment of their Article rights.

1. Right of access to one's own data

269. Individuals whose personal data has been collected and retained by the authorities have an interest, protected by Article 8, in receiving information: that was collected on them by the former secret services under totalitarian regimes and stored in State archives (*Haralambie v. Romania*, 2009, § 79; *Jarnea v. Romania*, 2011, § 50; *Joanna Szulc v. Poland*, 2012, § 87); that is necessary as regards their health or health risks to which they have been exposed (*Roche v. the United Kingdom* [GC], 2005, § 155; *K.H. and Others v. Slovakia*, 2009, § 44; *Yonchev v. Bulgaria*, 2017, § 46); to know and understand their childhood and early development (*Gaskin v. the United Kingdom,* 1989, § 41); or to trace their origins, and in particular their parents' identity (*Odièvre v. France* [GC], 2003, §§ 43-44; *Godelli v. Italy*, 2012, §§ 62-63; *M.G. v. the United Kingdom*, 2002, § 27).

270. In these different contexts the authorities have a positive obligation inherent in effective respect for private life, as secured under Article 8, to provide an effective and accessible procedure enabling the applicant to have access to all relevant and appropriate information required for specific purposes (*Roche v. the United Kingdom* [GC], 2005, § 162; *Haralambie v. Romania*, 2009, § 86; *Joanna Szulc v. Poland*, 2012, §§ 86, 94).

271. Conversely, where the State legitimately fears that access to information comprising personal data might jeopardise the efficacy of a secret surveillance system designed to protect national security or to combat terrorism, it can refuse access to the information collected and stored in a secret register

without breaching the positive obligation on the authorities under Article 8 (*Leander v. Sweden*, 1987, § 66; *Segerstedt-Wiberg and Others v. Sweden*, 2006, § 102). In order to determine whether the State is entitled to consider that the interests of national security and the fight against terrorism prevail over a person's interests in being advised of the full extent to which information was kept about them in the security services, the Court must be satisfied that there are sufficient safeguards against arbitrariness. The quality of the law (ibid., §§ 79-80) and the guarantees put in place, and in particular the possibility of reviewing the impugned measure and the remedies available to the data subject at the domestic level (ibid., §§ 52-68), are important criteria to be taken into account in balancing the competing interests (ibid., § 103). Similar principles are applicable in the context of expulsion of aliens. In *Hassine v. Romania*, 2021, §§ 55-69, the applicant, a Tunisian national lawfully resident in Romania, was expelled from the country on national-security grounds and declared an undesirable person in Romania for a five-year period on the basis of certain information from the Romanian intelligence services, which was classified as secret, and which allegedly suggested that he was engaged in activities capable of endangering national security. Neither the applicant nor his lawyer were authorised to consult those documents. The Court found that the administrative proceedings for the applicant's expulsion had lacked the necessary procedural safeguards and found a violation of Article 1 of Protocol No. 7.

272. In a case concerning the long-term registration of an applicant's personal data in the Schengen Information System, the Court ruled that the applicant's lack of full personal access to the information which he had requested could not breach the right to respect for his private life, having regard to the overriding need to protect national security (*Dalea v. France* (dec.), 2010). Whilst the applicant had not been in a position to challenge the precise grounds for his inclusion in the Schengen database, he had been granted access to all the other data concerning him and had been informed that considerations relating to State security, defence and public safety had given rise to the report (ibid., with reference to *Leander v. Sweden*, 1987, § 66).

273. Where only some of the documents in a file stored by the authorities on an individual, which included personal data, had been classified for State secrecy purposes, the authorities could have given the applicant partial access to the file (*Yonchev v. Bulgaria*, 2017, §§ 55-59). Thus, in a case concerning a refusal by the authorities to allow the applicant, a former police officer, to consult selected documents from his personal file, namely his psychological assessments, the Court found a violation of Article 8 on account of an overly formal domestic regulation requiring that where even one of the documents in a file was classified, the rest was automatically also to be considered classified and thus subject to the rules on the protection of classified information (ibid., § 60).

274. Where domestic legislation explicitly provided for a right of access to a personal file recorded and stored by the former security services under the totalitarian regimes in the former communist States, the State was required to put in place an effective and accessible procedure enabling the data subject to have reasonably prompt access to all relevant information (*Haralambie v. Romania*, 2009, § 86; *Jarnea v. Romania*, 2011, § 50; *Antoneta Tudor v. Romania*, 2013, § 34; *Joanna Szulc v. Poland*, 2012, §§ 86, 94). The Court found a violation of Article 8 in a case in which the applicant had only been given access to part of a file kept in his name, which had been recorded and stored by the former secret services (*Jarnea v. Romania*, 2011, §§ 54-60), and in two other cases in which the applicants had only been given access to their documents ten years after their initial request (*Joanna Szulc v. Poland*, 2012, §§ 93-95; *Antoneta Tudor v. Romania*, 2013, §§ 34-40). Defects in the archiving system or factual errors such as the registration of the wrong date of birth in an applicant's personal file could not justify a six-year delay in granting him access to his personal data (*Haralambie v. Romania,* 2009, § 95). The advanced age of a person requesting access to this type of information lent even greater urgency to his interest in tracing his personal history at the time of the totalitarian regime (ibid., § 93 *in fine*).

275. As regards information on health or health risks, the right of access to personal data extends to the making available to the data subject of copies of his or her data files (*K.H. and Others v. Slovakia*,

2009, § 47). It is for the file holder to determine the arrangements for copying personal data files and whether the cost thereof should be borne by the data subject (ibid., § 48). Data subjects should not be obliged to specifically justify a request to be provided with a copy of their personal data files. It is rather for the authorities to show that there are compelling reasons for refusing this facility (ibid., § 48). In the case of *K.H. and Others v. Slovakia*, 2009 (§§ 50-58), former hospital patients were unable to photocopy their original medical records, which had been collated and stored in a public hospital, including information which they considered important from the point of view of their moral and physical integrity. The Court found that the sole possibility offered by the hospital of making handwritten excerpts from the original files had not provided them with effective access to the relevant documents concerning their health.

276. Where a Government engages in hazardous activities which might have hidden adverse consequences on the health of those involved in such activities, the authorities have a 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 (*McGinley and Egan v. the United Kingdom*, 1998, § 101; *Roche v. the United Kingdom* [GC], 2005, § 161-162). An unreasonable waiting period, for example when health information and research services initiated the relevant document retrieval and disclosure procedures almost ten years after the applicant began seeking the documents in question, amounts to a failure on the part of the State, in breach of Article 8, to fulfil its positive obligation inherent in respect for the data subject's private life, notwithstanding the difficulties linked to the age and dispersed nature of the documents (ibid., § 166).

277. Aa regards access to the personal data of a person who, as a child, had been taken into care following the death of his parents or on account of their inability to look after him, a system which made access to the files subject to the agreement of the "contributors to the records", that is to say the persons having originated the relevant documents, may, in principle, be compatible with Article 8 under the State's margin of appreciation. However, such a system must protect the interests of anyone seeking to consult documents relating to his private and family life, and 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 (*Gaskin v. the United Kingdom*, 1989, § 49). In cases where the national system failed to provide for an appeal to such a body in the event of a refusal by the social services to grant access to all the documents in a given file, including where a third party concerned by or having originated the information withholds consent to disclosure, the Court has found a violation of Article 8 (ibid., § 49; *M.G. v. the United Kingdom*, 2002, §§ 30-32).

278. The Court takes the view that a child born out of wedlock who seeks a determination of the legal link with his biological father has a vital interest protected under the Convention in obtaining the information which he needs to learn the truth about an important aspect of his personal identity (*Mikulić v. Croatia*, 2002, § 64; *Boljević v. Serbia*, 2020, § 50). A system which has no means of compelling the alleged father to comply with a court order for DNA tests to be carried out, can in principle be considered compatible with the obligations deriving from Article 8, having regard to the State's margin of appreciation (*Mikulić v. Croatia*, 2002, § 64). However, the lack of any procedural measure to compel the alleged father to comply with the court order is only in conformity with the principle of proportionality if it provides alternative means enabling an independent authority to determine the paternity claim speedily (ibid., § 64). The Court found a violation of Article 8 in a case where, if the putative father refused to take part in the medical procedure, the national system provided for no measures to force him to submit to the DNA tests or alternative means enabling an independent authority to determine the paternity claim speedily (ibid., § 64). An individual's interest in discovering his parentage does not disappear with age, quite the reverse (*Jäggi v. Switzerland*, 2006, § 40, concerning a refusal to authorise DNA testing on a deceased person as requested by his alleged son, who wished to ascertain his legal descent; *Boljević v. Serbia*, 2020, § 54).

279. In the case of children born anonymously, the issue of access to one's origins and to information on the identity of one's biological parents is different from that of access to a case record concerning a child in care or to evidence of alleged paternity (*Odièvre v. France* [GC], 2003, § 43; *Godelli v. Italy*, 2012, § 62). Depending on the wide range of different legal systems and traditions, States had to benefit from a degree of discretion in preserving the confidentiality of the identities of biological parents (*Odièvre v. France* [GC], 2003, § 46; *Godelli v. Italy*, 2012, § 65). A national system which provided an applicant with access to non-identifying information on his mother and his biological family, enabling her to establish some her past history, without prejudice to third-party interests, accompanied by the possibility under recently enacted legislation to call on the services of an independent body mandated to help individuals to find their biological origins in order to secure the disclosure of her mother's identity, subject to the latter's consent, was deemed compatible with Article 8 (*Odièvre v. France* [GC], 2003, § 49). Conversely, a system which gave blind preference to a mother's wish to remain anonymous and provided no means for an adopted child who had not been recognised at birth of applying for either access to non-identifying information on her origins or disclosure of her mother's identity, was found to be incompatible with the requirements of Article 8 (*Godelli v. Italy*, 2012, §§ 70-72).

2. Right of rectification

280. The Court has examined several cases concerning the storage by the authorities of false data or data whose accuracy was disputed by the applicant (*Rotaru v. Romania* [GC], 2000, §§ 42-44, 55-63, concerning the applicant's inability to refute data regarding his alleged participation in the Romanian legionnaire movement in a file established by the security service; *Cemalettin Canlı v. Turkey*, 2008, §§ 34-37, concerning the inclusion in judicial proceedings of incomplete personal data collected by the police; *Khelili v. Switzerland*, 2011, § 56, concerning the retention in police files of an entry stating "prostitute" as the occupation of a person who had always denied having prostitute herself).

281. The inability of an individual to secure rectification of a report referring to him in the Schengen database (*Dalea v. France* (dec.), 2010) and the registration of a person's ethnic origin in official records (*Ciubotaru v. Moldova*, 2010, § 59) amount to interference with their right to respect for private life. In some circumstances, in particular where considerations of State security, national defence and public security are at stake, such interference is not necessarily incompatible with Article 8 (*Dalea v. France* (dec.), 2010). The existence of guarantees against arbitrariness and the ability to have the measure in question scrutinised by an independent and impartial body competent to review all the relevant questions of fact and law, in order to determine the lawfulness of the measure and censure a possible abuse by the authorities, are essential (ibid., referring to *Leander v. Sweden*, 1987, § 66).

282. False or incomplete personal information collected and retained by the authorities may make everyday life difficult for the data subject (*Khelili v. Switzerland*, 2011, § 64), prove defamatory (*Rotaru v. Romania* [GC], 2000, § 44) or remove a number of substantial procedural safeguards provided by law to protect the rights of data subjects (*Cemalettin Canlı v. Turkey*, 2008, §§ 35, 40-42). In a case in which a police file headed "information note on other offences" had been presented before a domestic court mentioning two criminal actions brought against the defendant in the past for membership of illegal organisations, the Court found a violation of Article 8. In this case not only had the information set out in the file been false, but also the file had failed to mention the applicant's acquittal during the first criminal action and the discontinuance of proceedings during the second one (ibid., § 42). The failure to mention the outcome of the two sets of proceedings had been contrary to the obligations unequivocally set out in domestic regulations, thus removing a number of substantial procedural safeguards laid down by law to protect the applicant 's rights (ibid., 2008, § 42).

283. The fact of imposing on an individual requesting rectification of his personal data in the official State registers a requirement which creates insurmountable barriers for him may prove incompatible with the State's obligation to guarantee effective respect for his private life (*Ciubotaru v. Moldova*,

2010, §§ 51-59). In a case concerning the applicant's inability to obtain the modification of the registration of his ethnic origin in the official registers, the requirement on proving that his parents had belonged to a specific ethnic group had created insurmountable barriers for the data subject in recording an ethnic identity different from that recorded in respect of his parents by the authorities (ibid., § 57).

284. In the context of requests for rectification of civil status registers to take into account the post-operative status of a transsexual person, the coherency of administrative and legal practices within the domestic system must be regarded as an important factor in the assessment of such requests carried out under Article 8 (*Christine Goodwin v. the United Kingdom* [GC], 2002, § 78). In a case concerning a refusal by the authorities to modify the birth register, the Court stated that it was struck by the fact that the gender reassignment which is lawfully provided is not met with full recognition in law, which might be regarded as the final and culminating step in the long and difficult process of transformation which the transsexual has undergone (ibid., § 78, reversing its case-law to take account of developments in science and society since the time of such older judgments as *Rees v. the United Kingdom*, 1986, §§ 42-44, *Cossey v. the United Kingdom,* 1990, §§ 39-40, and *Sheffield and Horsham v. the United Kingdom* [GC], 1998, §§ 60-61). Where a State has authorised the treatment and surgery alleviating the condition of a transsexual, financed or assisted in financing the operations and indeed permits the artificial insemination of a woman living with a female-to-male transsexual, it appears illogical to refuse to recognise the legal implications of the result to which the treatment leads (*Christine Goodwin v. the United Kingdom* [GC], 2002, § 78), especially since the difficulties posed by the rectification of an initial gender entry in the birth register are far from insurmountable (ibid., § 91).

285. In the case of *S.V. v. Italy*, 2018 (§ 72), a refusal by the authorities to authorise a change of forename for a transsexual person during the gender transition process and before completion of the gender reassignment operation had been based on rigid judicial proceedings which had placed the applicant for an unreasonable length of time (two-and-a-half years) in an anomalous position in which she was apt to experience feelings of vulnerability.

286. In the case of *Hämäläinen v. Finland* [GC], 2014 (§§ 87-89), the Court considered that it had not been disproportionate to require, as a precondition to legal recognition of an acquired gender, that the applicant's marriage be converted into a registered partnership, as that was a genuine option which provided legal protection for same-sex couples that is almost identical to that of marriage (homosexual marriage being illegal in Finland). Consequently, the minor differences between these two legal concepts were not such as to render the current Finnish system deficient from the point of view of the State's positive obligation. See also *A.P., Garçon and Nicot v. France*, 2017, concerning the legal conditions for a civil status change in respect of transgender persons, such as the irreversible nature of the change in their appearance (§§ 116-135), the reality of the gender identity disorder (§§ 138-144) and the obligation to undergo a medical examination (§§ 149-154).

3. Right to data deletion ("right to be forgotten")

287. The Court has dealt with the issue of the right to deletion of personal data ("the right to be forgotten") after a specific period of time as regards:

- a media choice or practice of leaving on their websites archives comprising personal data on individuals such as their surnames, forenames and photographs, which had been published in the past (*M.L. and W.W. v. Germany*, 2018);
- the ability of individuals accused, or merely suspected, of committing an offence to obtain, after a certain lapse of time, the removal of their personal data (DNA profile, identity photographs and fingerprints) collected by the authorities in databases aimed at preventing and fighting crime (*B.B. v. France*, 2009; *Gardel v. France*, 2009; *M.B. v. France*, 2009; *M. K. v. France*, 2013; *Brunet v. France*, 2014; *Ayçaguer v. France*, 2017; *Catt v. the United Kingdom*, 2019; *Gaughran v. the United Kingdom*, 2020);

- an individual's inability to obtain the removal of his previous convictions from his police record after a specific period of time (*M.M. v. the United Kingdom*, 2012);
- the protracted retention in the security service archives of the applicants' personal data, which no longer complied with the requirement of "necessity in a democratic society" in view of their nature and age (*Segerstedt-Wiberg and Others v. Sweden*, 2006).

288. In the context of media web archives comprising the personal data of an individual who had been the subject of a publication in the past, the "right to be forgotten" is intended to protect a data subject by enabling him to request the partial or complete deletion of the search results linked to his name which he deemed inappropriate after a certain lapse of time (*M.L. and W.W. v. Germany*, 2018, § 100). That right is not absolute. However important it might be, it must be balanced against the general public's right to be informed of past events and about contemporary history, particularly by means of press digital archives (ibid., § 101). In addition to the primary function of the press in imparting information and ideas of general interest, the press has a secondary but nonetheless valuable role in maintaining archives containing news which has previously been reported and making them available to the public (ibid., § 90). Internet archives make a substantial contribution to preserving and making available news and information. Digital archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free (ibid., § 90, and the references therein).

289. In the case of *M.L. and W.W. v. Germany*, 2018, two individuals who had been convicted of murder and been released fourteen years later, having served their prison sentence, unsuccessfully requested that the newspaper web archives remove their photographs and statements of their full identities (surnames and forenames) to enable them to make a new start in life out of public view. The Court found no violation of Article 8 on the grounds that the public interest in having access to accurate and objective archives should take precedence (ibid., § 116).

290. The judgment in the case of *M.L. and W.W. v. Germany*, 2018, sets out a series of pointers on the scope of the "right to be forgotten" in the context of media web archives comprising individuals' personal data.

- In the Court's view, it would be too complicated for the media to have systematically to introduce procedures for accepting requests for anonymity or at least for assessing them in line with criteria based on precedent. Such an obligation poses the risk of the press refraining from retaining reports in its online archives or omitting identifying information from its reports which is liable to become the subject of such requests (ibid., § 103).
- An obligation on journalists to render a report anonymous is less detrimental to freedom of expression than the deletion of an entire report (ibid., § 105, and the references therein). However, the approach to covering a given subject is a matter of journalistic freedom, and Article 10 of the Convention leaves it to journalists to decide what details ought to be published in order to ensure an article's credibility, provided that the choices which they make in that regard are based on their profession's ethical rules and codes of conduct. The inclusion in a report of individualised information such as the full name of the person concerned is an important aspect of the press's work, especially when reporting on criminal proceedings that have attracted considerable interest.
- A convicted person's behaviour going far beyond the mere use of the remedies available under domestic criminal law to challenge his conviction may limit their legitimate expectation of obtaining anonymity in the reports or even a right to be forgotten online, even as their release approaches (ibid., § 109).
- The manner in which the report or photograph is published and in which the person concerned is presented therein, as well as the extent of the dissemination of the report or photograph, can be taken into account (ibid., § 110). Images showing an individual as he had

appeared thirteen years previously had reduced the likelihood of their being recognised by third parties on the basis of the photos (ibid., § 115).

291. In *M.M. v. the United Kingdom*, 2012 (§§187-207), the lifelong registration of a caution in a person's police record led to a finding of a violation of Article 8. The Court considered that a conviction or a caution issued to an individual in the past became, with the passage of time, an integral part of his or her private life, which had to be respected. Even though the data on the criminal record was, in a sense, public information, its systematic storage in central files meant that it could be disclosed long after the event, when everyone except the data subject would probably have forgotten the incident. The Court deemed disquieting the fact that the criteria for review to enable the data to be deleted had been very restrictive, and that requests for deletion were allowed only in exceptional cases (ibid., § 202).

292. The Court holds that where a State pushes its margin of appreciation to the extremes by maximising its powers in the sphere of data retention, that is, by storing data indefinitely, it is decisive that there should be effective safeguards providing for the deletion of personal data when their continued retention has become disproportionate (*Catt v. the United Kingdom*, 2019, § 119; *Gaughran v. the United Kingdom*, 2020, § 94). In a case in which the biometric data and photographs of the applicant, who had been convicted of driving with excess alcohol, had been retained under a policy of indefinite storage of the personal data of anyone found guilty of a criminal offence, the Court found a violation of Article 8 (ibid., § 98). There was no provision allowing the applicant to apply to have the data concerning him deleted if conserving the data no longer appeared necessary in view of the nature of the offence, the age of the person concerned, the length of time that has elapsed and the person's current personality. The police could only delete the biometric data and photographs of convicted persons in exceptional cases. Review possibilities were so narrow as to be almost hypothetical (ibid., § 94).

293. The lack of effective safeguards on deletion of personal data which are no longer relevant in terms of the purpose of their storage is particularly worrying in the case of special categories of sensitive data attracting a heightened level of protection (*Catt v. the United Kingdom*, 2019, § 112). In a case concerning the retention in a police database of sensitive data relating to a peaceful demonstrator, revealing his political opinions, the Court found a violation of Article 8 (ibid., § 128). In the absence of any regulations on the maximum period of storage of such data, the applicant was left entirely dependent on the diligence with which the authorities would apply the guarantees set out in the applicable code of practice, which were very flexible, in order to ensure the proportionality of the period of retention of his data. The Court held that the guarantee of obtaining the deletion of the data had a limited effect where the authorities refused, following a request from the data subject, to delete the data in question or to give reasons for their decision to retain them (ibid., §§ 118 and 122).

294. In several cases relating to the retention of the personal data of individuals convicted of sexual assault, the Court found no violation of Article 8 after noting that the data subjects had been able to submit a request for deletion if the retention of their data no longer seemed relevant in view, *inter alia*, of the lapse of time since their conviction (*B.B. v. France*, 2009, §§ 66-68; *Gardel v. France*, 2009, §§ 67-69; *M.B. v. France*, 2009, §§ 58-60).

295. In the case of *Peruzzo and Martens v. Germany* (dec.), 2013 (§ 46), concerning the storage of personal data in a file following a conviction for serious offences linked to drug trafficking, the Court was satisfied that although the law had prescribed no maximum periods for the storage of DNA profiles, the Federal Criminal Office had been required to check at regular intervals of no more than 10 years whether the data storage was still necessary, having regard in each case to the purpose of the data retention and the nature and gravity of the circumstances of the case.

296. In *Ayçaguer v. France*, 2017 (§ 44), the Court found a violation of Article 8 because, owing to its duration and the impossibility of deletion, the current regulations on the storage of DNA profiles in the national database, to which the applicant had objected by refusing to undergo sampling, did not

provide the data subject with sufficient protection (ibid., § 45). The Court emphasised that convicted persons should, like persons who were suspected of committing a criminal offence, discharged or acquitted, be given a concrete opportunity to submit a request for the deletion of stored data, so as to ensure that the period of data retention is proportionate to the nature of the offences and the aims of the restrictions (ibid., § 45; *B.B. v. France*, 2009, § 68; *Brunet v. Francee*, 2014, §§ 41-43).

297. In connection with the possibility of deleting personal data, the right at any time to submit a deletion request to the court is liable to conflict with the interests of the investigating authorities, which require access to a database with as many references as possible. Accordingly, since the interests at stake are contradictory, if only partially, the deletion provides a safeguard which is "theoretical and illusory" rather than "practical and effective" (*M. K. v. France*, 2013, §§ 44-47).

298. In the case of *Segerstedt-Wiberg and Others v. Sweden*, 2006 (§§ 73-92), the storage in the files of the State security services of very old personal data relating to the applicants' attendance at a political meeting, the fact that they had advocated violent resistance to police checks during demonstrations, and their membership of a specified political party, had amounted to a violation of Article 8. The Court considered that the State's interest in protecting national security and fighting terrorism, justifying the collection and storage of the information in question, should be balanced against the seriousness of the interference in the exercise by each of the applicants of their right to respect for their private life. In view of the nature and age of the information on the applicants, the reasons behind its storage, although relevant, could not be deemed sufficient thirty years later (ibid., § 90).

299. In the context of Article 10, the Court has dealt with "the right to be forgotten" in the case of *Mediengruppe Österreich GmbH v. Austria*, 2022, which concerned a court order requiring a daily newspaper not to publish particular information about an individual indirectly connected to the campaign of a political candidate in the run-up to a presidential election. The newspaper had published a photo of the brother of the candidate's office manager in a "right-wing scene" and had revealed that he was a "convicted neo-Nazi". Over twenty years had passed between that conviction and the publication of the article at issue, and some seventeen years since his release from prison: moreover, the conviction had already been deleted from his criminal record at the time of the publication in question. The national superior court pointed to a lack of a temporal connection and prohibited the applicant company from publishing pictures of the office manager's brother without his consent if reporting in the same article that he was a convicted neo-Nazi in the accompanying report. The Court has found no violation of Article 10, emphasising, in particular, the lapse of time between the conviction, the release and the publication of the article in question; the loss of notoriety of the person concerned; the fact that he had no further criminal conviction; the importance of reintegration into society of persons who have served their sentence; and their legitimate and very significant interest in no longer being confronted with their conviction after a certain period of time.

4. Right to benefit from special procedural safeguards and an effective procedural framework to uphold one's rights

300. Even though Article 8 contains no explicit procedural requirements, it is important for the effective enjoyment of the rights guaranteed by this provision that the relevant decision-making process is fair and such as to afford due respect to the interests safeguarded by it. Such a process may require the existence of an effective procedural framework whereby an applicant can assert his or her rights under Article 8 under conditions of fairness, including as regards matters of proof and evidence (*I. v. Finland*, 2008, § 44; *Ciubotaru v. Moldova*, 2010, § 51). The fact of imposing a requirement which creates an insurmountable barrier for a person requesting rectification of his identity data in the official State registers may be incompatible with the State's positive obligation to guarantee effective compliance with the right to respect for his private life (ibid., §§ 51-59). In a case concerning the disclosure of the applicant's HIV-positive status, the Court, finding a violation of Article 8, attached

weight to the fact that the State had imposed an excessively heavy burden of proof on the applicant in the framework of civil proceedings during which she had claimed compensation for the dissemination of information on her state of health (*I. v. Finland*, 2008, § 44).

301. Restrictions imposed by law on the domestic courts' powers to compensate for damage caused by the press disclosure of confidential information on the health of identified persons and to deter the recurrence of such abuses were liable to hamper the effectiveness of any appeal, thus failing to provide the applicants with such protection of their private life as they might legitimately have expected. Thus, in *Armonienė v. Lithuania*, 2008 (§§ 47-48) and *Biriuk v. Lithuania*, 2008 (§§ 46-47), the Court found a violation of Article 8 because the Law on Provision of Information to the Public in force at the material time had set an upper limit on damages awarded to the applicants by the domestic courts following the disclosure of their HIV-positive status in the leading national daily newspaper, without their consent and revealing their identities.

302. The failure of the State to provide, at the national level, for independent review of the justification of the retention of personal data collected in the framework of criminal proceedings or following criminal proceedings in which the defendant was acquitted, discharged or convicted, is an important aspect which must be taken into account in determining whether such data retention is compatible with Article 8 (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 119, 125). In a case concerning the indefinite retention of cellular samples, DNA profiles and fingerprints from two individuals after the criminal proceedings against them had concluded with an acquittal and a discharge, respectively, the Court found a violation of Article 8 on noting that the applicants had stood little chance of securing the removal of the data from the national database or the destruction of the samples.

303. In the case of *Vicent Del Campo v. Spain*, 2018 (§§ 39, 53), the inability of the applicant, a third party in judicial proceedings, to apply to a national court to refrain from communicating his identity or personal information concerning him before delivery of a judgment, had deprived him of an effective procedural framework for defending his rights.

304. The authorities' failure to carry out a proportionality analysis of the competing interests at stake and to give consideration to the applicant's privacy rights and to data protection issues will fall foul of the requirements of Article 8 of the Convention (*Liebscher v. Austria*, 2021, §§ 64-69).

305. In *M.D. and Others v. Spain*, 2022 (§§ 65-72) concerning the leak to the press of the applicants' personal data from the police database to which only the authorities had access, the Court held, as regards such an unlawful disclosure of private data retained by public organs, that the positive obligation under Article 8 implied an "obligation to carry out effective inquiries" in order to determine the circumstances in which the journalists had gained access to the data and, if necessary, to sanction the persons responsible for the shortcomings that had occurred. The authorities' failure to carry out such inquiries amounted to a breach of Article 8. Likewise, in *Y.G. v. Russia*, 2022, (§§ 46-53), where the applicant complained that a database containing his personal data, including information on his health status, had been available for sale at a market, the Court considered that in the face of such a major privacy breach, the applicant acting on his own, without the benefit of the State's assistance in the form of an official inquiry, had no effective means of establishing the perpetrators of those acts so that his criminal-law complaint had not been an inappropriate avenue in those circumstances. By failing to carry out an investigation, the authorities breached their positive obligation to ensure adequate protection of his right to respect for his private life.

306. The effectiveness of remedies available at the domestic level for persons wishing to have access to their personal data requires applications submitted by the data subjects to be processed within a reasonable time. In the case of *Roche v. the United Kingdom* [GC], 2005 (§§ 166-167, 169), the Court found a violation of Article 8 on account of an unreasonable waiting period for the applicant in accessing documents comprising personal data which would have enabled him to assess the potential risks to his health caused by his participation in military testing on gases.

307. Excessive importance attached by the domestic authorities to the requirement of confidentiality *vis-à-vis* Internet users' traffic data may, under certain circumstances, prove contrary to Article 8 if it hampers the effectiveness of a criminal investigation aimed at identifying and punishing an offender (*K.U. v. Finland,* 2008, § 49). In *K.U. v. Finland*, 2008 (§§ 49-50), the Court found a violation of Article 8 in the absence of a procedural framework enabling the identification and bringing to justice of a person who had published an advert on Internet making a minor a target for approaches by paedophiles, so as to enable the victim to claim pecuniary redress from the person in question. The guarantee enjoyed by users of telecommunications and Internet services concerning respect for their privacy is sometimes outweighed by other legitimate concerns such as the prevention of disorder and crime or the protection of the rights and freedoms of others.

308. In the national security sphere, anyone who is the subject of a measure for the aforementioned reasons must be able to obtain the review of the impugned measure by an independent and impartial body empowered to consider all the relevant factual and legal issues and if necessary to penalise any abuse committed by the authorities. Before such a review body the persons concerned must benefit from adversarial proceedings enabling them to present their point of view and refute the arguments put forward by the authorities. Thus, in the case of *Dalea v. France* (dec.), 2010, the Court considered that the protracted registration of the applicant's personal data in the Schengen database could be deemed "necessary in a democratic society" because he had benefited from a review of the impugned measure. Even though he had not been able to object to the specific reason for the registration of his data, he had had cognisance of all the other data concerning him in the Schengen database.

309. The independent and impartial body to which anyone who is the subject of a measure for national security reasons must be able to apply for a review of the impugned measure does not have to be have judicial status. In *Leander v. Sweden*, 1987 (§ 59), concerning the use of a secret police file to recruit a carpenter, the Court found no violation of Article 8 owing to the existence of guarantees, including the possibility of Parliament and independent institutions conducting a review of the operations authorising the relevant domestic authorities to collect and store in secret files information on individuals and then to use them (ibid., § 65), even though the applicant had not been entitled to a judicial remedy (ibid., §§ 62, 67). In order to assess the effectiveness of a remedy before a body responsible at the domestic level for reviewing a measure based on reasons of national security, regard must be had to the procedural powers and guarantees implemented by the body in question (ibid., §§ 77, 80, 83-84). A hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the requisite standards of independence needed to constitute sufficient protection against the abuse of authority (*Roman Zakharov v. Russia* [GC], 2015, § 292).

310. In the framework of secret surveillance measures, review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his rights. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (ibid., § 233; *Klass and Others v. Germany*, 1978, §§ 55-56).

311. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers (*Roman Zakharov v. Russia* [GC], 2015, § 234). There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his

knowledge and thus able to challenge their legality retrospectively (*Klass and Others v. Germany*, 1978, §§ 57-59; *Weber and Saravia v. Germany* (dec.), 2006, §§ 135-137), or if any person who suspects that his communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications (*Kennedy v. the United Kingdom*, 2010, §§ 167, 169; *Roman Zakharov v. Russia* [GC], 2015, § 234).

312. In the cases of *Klass and Others v. Germany*, 1978 (§§ 57-59) and *Weber and Saravia v. Germany* (dec.), 2006 (§§ 135-137), the Court found that the remedies available at the domestic level had been adequate. The individuals whose communications had been monitored had been notified as soon as possible, without jeopardising the aim of the monitoring. The remedies had also been surrounded by effective safeguards, such as the fact that an independent body was empowered to decide whether a person being monitored should be notified of the measure. Relying on that notification, the person had various judicial options, for example bringing a civil action for damages or an application to the Federal Constitutional Court for a ruling on a possible violation of the Basic Law (*Klass and Others v. Germany*, 1978, §§ 57, 24).

313. For systems which do not provide for notification of the person concerned of the measures taken against him, the fact that the individuals concerned consider that their right to respect for their private lives has been infringed by a secret monitoring measure can apply to an independent and impartial body even if they were not informed in advance that their communications had been intercepted was considered by the Court as providing an important safeguard, in a case in which it found no violation of Article 8 (*Kennedy v. the United Kingdom*, 2010, §§ 167, 169). Conversely, where the remedies available under the domestic system are open solely to persons with a minimum of information on the impugned measure, the Court held that those concerned had not had an effective remedy against the secret monitoring measures, in breach of Article 8 (*Roman Zakharov v. Russia* [GC], 2015, §§ 293-298, 305).

III. Interaction with other provisions of the Convention and its Protocols

314. Besides the right to respect for private and family life, the home and correspondence guaranteed by Article 8 of the Convention, which is the primary source of protection of personal data in the Convention system, issues linked to that protection may also come into play under other provisions of the Convention and its Protocols. In such cases the Court's main task is to weigh up this protection and reconcile it with other rights and legitimate interests. In some cases the issue of protection of personal data has enabled the Court to determine the scope of another right guaranteed by the Convention and its additional Protocols.

A. Data protection and substantive rights[10]

Article 9 of the Convention

"1. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.

2. Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others."

Article 10 of the Convention

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Article 14 of the Convention

"The enjoyment of the rights and freedoms set forth in [the] Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

Article 1 of Protocol No. 1

"Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

[10] This chapter should be read in the light of and in conjunction with the Guide on Article 9, the Guide on Article 10, the Guide on Article 14 and Article 1 Protocol No. 12 and the Guide on Article 1 of Protocol No. 1.

Article 2 of Protocol No. 4

"1. Everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence.

2. Everyone shall be free to leave any country, including his own.

3. No restrictions shall be placed on the exercise of these rights other than such as are in accordance with law and are necessary in a democratic society in the interests of national security or public safety, for the maintenance of *ordre public*, for the prevention of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4. The rights set forth in paragraph 1 may also be subject, in particular areas, to restrictions imposed in accordance with law and justified by the public interest in a democratic society."

1. Data protection and freedom of thought, conscience and religion (Article 9 of the Convention)

315. The Court has found a violation of Article 9 in some cases that also raise the issue of personal data protection, while in other cases finding no violation.

316. In the case of *Sinan Işık v. Turkey*, 2010 (§§ 37-53), the Court was faced with the issue of the indication – whether obligatory or optional – of the applicant's religion on his identity card. In the Court's view, the fact of having to apply to the authorities in writing to have the indication of religion changed in the civil registers and on identity cards, and similarly, the mere fact of having an identity card with the "religion" box left blank, obliged the individual to disclose, against his or her will, information concerning an aspect of his or her religion or most personal convictions. The Court found a violation of Article 9 after reiterating that the freedom to manifest one's religion or beliefs also had a negative aspect, namely an individual's right not to be obliged to disclose his or her religion or to act in such a way that it was possible to conclude that he or she held – or did not hold – such beliefs. Even though the religion box could be left blank, the very fact of doing so in itself had a specific connotation, as it would inevitably allow a distinction to be made between the bearers of identity cards containing the information in question and those who had chosen not to indicate it (ibid., § 51).

317. In *Alexandridis v. Greece*, 2008 (§ 41), the requirement for a lawyer to reveal to the court that he was not an Orthodox Christian, and that he wanted to make a solemn declaration rather than take the religious oath, had interfered with his Article 9 rights. The State authorities did not have the right to intervene in the sphere of individual conscience and to ascertain individuals' religious beliefs or oblige them to reveal their beliefs concerning spiritual matters. This was all the more true in cases where a person was obliged to take such action with a view to performing certain duties, in particular when taking an oath (ibid., § 38). In the case of *Dimitras and Others v. Greece*, 2010 (§ 88), the requirement for the applicants to reveal their religious beliefs in order not to take a religious oath as witnesses in criminal proceedings was also found to be in breach of Article 9. The Court considered that the provisions of the Code of Criminal Procedure which stipulated that, for the purpose of verifying their identity, all witnesses were required, amongst other information, to state their religion before testifying were difficult to reconcile with freedom of religion (ibid., § 88).

318. In the case of *Mockutė v. Lithuania*, 2018 (§ 129), the Court was prepared to accept that the needs of psychiatric treatment might make it necessary for a psychiatrist to discuss various matters, including religion, with a patient. However, such discussions should not take the form of psychiatrists prying into patients' beliefs in order to "correct" them when there was no clear and imminent risk that such beliefs would manifest in actions dangerous to the patient or others. A State could not dictate what a person believed or take coercive steps to make him change his beliefs, nor could the scope of

the States' margin of appreciation be broader or narrower depending on the nature of the religious beliefs.

2. Data protection and freedom of expression (Article 10 of the Convention)[11]

319. As a general rule, in cases in which the Court has had to weigh up and reconcile the right to the protection of personal data as guaranteed by Article 8 and the right to freedom of expression under Article 10, it has found that the outcome should not, in principle, vary according to whether the application was lodged under Article 8 or under Article 10. In the Court's view, the two rights merit equal respect (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 163; *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, 2018, § 46).

320. The refusal by the authorities to provide non-governmental organisations with access to certain information containing personal data held by the State was found to be in breach of Article 10 in the following cases:

- *Centre for Democracy and the Rule of Law v. Ukraine*, 2020 (§§ 120-121), concerning the refusal of the Central Election Commission to provide an NGO with copies of the CVs of the leaders of the political parties standing as candidates in the parliamentary elections, on the grounds that the information requested was confidential and could only be disclosed in its entirety with the consent of the persons concerned;
- *Magyar Helsinki Bizottság v. Hungary* [GC], 2016 (§§ 195-197, 200), where the authorities had refused to provide an NGO carrying out a survey with the names of *ex officio* appointed defence counsel and the number of their respective appointments;
- *Youth Initiative for Human Rights v. Serbia*, 2013 (§§ 24-26), regarding the refusal of an intelligence agency to provide information to an NGO despite being ordered to do so.

321. With regard to the disclosure of personal data in the printed or audiovisual media, the Court has found a violation of Article 10 in a number of cases including:

- *N. Š. v. Croatia*, 2020 (§§ 92-117), where the applicant was convicted for disclosing on television supposedly confidential information she had obtained during administrative proceedings concerning custody of a child. The Court held that, owing to children's vulnerability, the protection of their personal data was essential (ibid., § 99). However, the unduly formalistic approach taken by the national courts, which did not take account of the background to the disclosure and in particular the fact that the information was already in the public domain, was incompatible with Article 10 (ibid., §§ 115-116);
- *Gîrleanu v. Romania*, 2018 (§§ 68-100), concerning an order for the applicant to pay an administrative fine for disclosing confidential military information as part of a journalistic investigation;
- *Couderc and Hachette Filipacchi Associés v. France* [GC], 2015 (§§ 94-153), on the subject of a court ruling against the publication director and the publisher of a weekly magazine for publishing an article and photographs revealing the existence of a monarch's secret child;
- *Axel Springer AG v. Germany* [GC], 2012 (§§ 75-111), concerning a ban on reporting on the arrest and conviction of a well-known actor;

[11] This chapter should be read in the light of and in conjunction with the Guide on Article 10 (see, in particular, pp. 26-47; 58-60 and 62-65).

- *Dupuis and Others v. France*, 2007 (§§ 30-32, 39-49), concerning the conviction of journalists for using and reproducing in their book information from the case file of an ongoing judicial investigation, including personal data of the accused.

322. Conversely, the Court has found no violation of Article 10 in several cases including:

- *Biancardi v. Italy,* 2021 (§§ 67-71) on the compatibility with Article 10 of a civil judgment against a journalist for not de-indexing sensitive information published on the Internet concerning criminal proceedings against a private individual and the journalist's decision to keep the information easily accessible in spite of the individual's opposition;
- *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 (§§ 139-199), concerning a judicial decision banning the mass publication of personal taxation data;
- *Bédat v. Switzerland* [GC], 2016 (§§ 44-82), on the conviction of a journalist for publishing information covered by the secrecy of criminal investigations;
- *Mediengruppe Österreich GmbH v. Austria*, 2022 (§§ 44-73), concerning a court order for a daily newspaper not to publish a photograph with a "convicted neo-Nazi" caption as regards an individual indirectly connected to the campaign of a political candidate in the run-up to a presidential election, the relevant publication having taken place more than twenty years after the conviction;
- *Gafiuc v. Romania*, 2020 (§§ 85-90), concerning the withdrawal of a journalist's accreditation to search the Securitate archives, following the disclosure in several articles written by him of personal data in "raw" form concerning various well-known sports figures, without the relevance of the data having been assessed in the light of the declared subject of his research, namely sport in Romania under the communist regime;
- *Giesbert and Others v. France*, 2017 (§§ 77-103), concerning the courts' findings against a newspaper for publishing documents from a set of criminal proceedings before they were to be read out at a public hearing;
- *Verlagsgruppe Droemer Knaur GmbH & Co. KG v. Germany*, 2017 (§§ 36-62), concerning an order for a publishing company to pay damages for failing to carry out thorough research and for serious interference with an individual's personality rights;
- *Kurier Zeitungsverlag und Druckerei GmbH v. Austria*, 2012 (§§ 47-56), concerning the requirement to pay compensation to a child who had been the victim of sexual abuse and whose identity was disclosed in a press article. In view of the vulnerability of crime victims, their identity deserved particular protection;
- *MGN Limited v. the United Kingdom*, 2011 (§ 152), in which the Court was persuaded, among other considerations, by the fact that the disclosure in the press of details of a celebrity's therapy for drug addiction was harmful and risked causing a significant setback to her recovery;
- *Editions Plon v. France*, 2004 (§§ 22-55), on the definitive suspension of distribution of a book containing information relating to a deceased Head of State and covered by medical confidentiality.

323. On the subject of the distribution of personal images in the press or the broadcasting media, and court orders banning the distribution of such personal data, the Court has found a violation of Article 10 in several cases including: *Pinto Coelho v. Portugal (no. 2)*, 2016 (§§ 31-56), concerning the conviction of a journalist for broadcasting a recording of a court hearing without permission; *Haldimann and Others v. Switzerland*, 2015 (§§ 63-68), in which four journalists, pursuing an aim in the public interest, were convicted for recording and broadcasting an interview with a private insurance broker using a hidden camera; *Krone Verlag GmbH & Co. KG v. Austria*, 2002, (§§ 21-39), concerning an injunction to refrain from publishing the picture of a politician; and *News Verlags GmbH*

& Co. KG v. Austria, 2000 (§§ 37-60), on an order banning a newspaper from publishing the photograph of a suspect in criminal proceedings.

324. However, the distribution of such images, or orders to refrain from distributing them, were found not to breach Article 10 in the following cases: *Société de Conception de Presse and d'Édition v. France*, 2016 (§§ 32-54), concerning a court order to black out a photograph in a magazine already on sale of a person who had been held captive and tortured; *Axel Springer SE and RTL Television GmbH v. Germany*, 2017 (§§ 43-59), relating to the decision to ban the publication of images that would have enabled a person on trial for murder to be identified; *Egeland and Hanseid v. Norway*, 2009 (§§ 56-65), concerning the conviction of the editors-in-chief of two newspapers for publishing photographs of a person about to be taken to prison to begin serving a lengthy sentence. See also paragraphs 17 and 65 above concerning the case of *Vučina v. Croatia* (dec.) 2019.

325. In the case of *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, 2018 (§§ 59-69, 77-78), the distribution for journalistic purposes of several videos filmed with a hidden camera as part of the covert surveillance of a public figure led to one finding of a violation and another finding of no violation of Article 10, depending on whether the recording had been made in a public or a private space.

326. With regard to the posting on the Internet by private individuals of images of other individuals filmed in secret, without the consent of the data subject, the Court found in the case of *Khadija Ismayilova v. Azerbaijan*, 2019 (§§ 158-166), that the respondent State had failed to protect the applicant, a journalist who had been filmed by unknown individuals using hidden cameras installed in her apartment. The unjustified public disclosure by the authorities, in a press release purporting to provide an update on a criminal investigation, of personal details such as the applicant's name and the addresses of her friends and colleagues had further compounded the situation, contrary to the spirit of an environment protective of journalism (ibid., § 165).

327. In a case concerning protection of the freedom of expression of a whistleblower and the disclosure of confidential information affecting State security, the Court found a violation of Article 10 on account of the applicant's conviction for making public a number of irregularities in the gathering of personal data by the intelligence service which he had identified in the course of his professional activity (*Bucur and Toma v. Romania*, 2013, §§ 95-120). In another whistleblower case, a deputy chief physician in a public hospital had been dismissed after he had reported his suspicions, later found to be groundless, of active euthanasia by his superior. The Court found no violation of Article 10: the applicant had based his suspicions on the information available in the electronic medical files (which, as he knew, did not contain all information on the patients' health) and not in the paper files (which contained all information). Thus, although he had acted in good faith, he had failed to carefully verify that the disclosed information was accurate and reliable (*Gawlik v. Liechtensten*, 2021, §§ 74-78).

328. The issue of the protection of journalists' personal data or of data in their possession that could result in their sources being identified has been examined by the Court in a number of cases including:

- *Sedletska v. Ukraine*, 2021 (§§ 59-60 and 64-73), where judicial authorisation given to the investigative authorities to access and collect a journalist's communications data – dates, times and location of her mobile phone near the specified streets and places over a sixteen-month period – stored by her mobile phone operator, was found to be in breach of Article 10 as it was not justified by an "overriding requirement in the public interest" and lacked procedural safeguards;
- *Jecker v. Switzerland*, 2020 (§§ 37-43), where an order for a journalist to disclose the identity of one of her sources, so as to help the prosecuting authorities to identify a drug dealer, was found by the Court to be contrary to Article 10 in the absence of any balancing of the specific interests at stake;
- *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, 2012 (§ 102), in which the placement of journalists under surveillance without prior review by an

independent body, and the order to surrender documents capable of leading to the identification of their sources, were found to be in breach of Articles 8 and 10 taken together. A review *post factum* would not have sufficed since the confidentiality of journalistic sources could not be restored once it had been destroyed (ibid., §§ 100-101);

- *Financial Times Ltd and Others v. the United Kingdom*, 2009 (§ 63), in which the Court specified that the conduct of the source could never be decisive in determining whether a disclosure order ought to be made but would merely operate as one, albeit important, factor to be taken into consideration in carrying out the balancing exercise required;
- *Weber and Saravia v. Germany* (dec.), 2006 (§§ 143-153), where the Court declared manifestly ill-founded a complaint alleging a breach of freedom of expression arising out of the provisions of a law authorising strategic monitoring of telecommunications and making it impossible for journalists to guarantee that the information they received in the course of their work remained confidential;
- *Ernst and Others v. Belgium*, 2003 (§§ 94-105), where searches and seizures on a large scale at the office of journalists, aimed at identifying their sources, were found to be in breach of Article 10. (See also the cases of *Roemen and Schmit v. Luxembourg*, 2003, §§ 47-60, concerning searches of a journalist's home aimed at identifying his sources; *Tillack v. Belgium*, 2007, §§ 56-68, concerning search and seizure operations carried out at the home and office of a journalist suspected of bribing a European civil servant in order to obtain confidential information about investigations in progress in the European institutions, with a view to identifying the source of the disclosures; *Sanoma Uitgevers B.V. v. the Netherlands* [GC], 2010, §§ 64-100, relating to the seizure by police of documents that would have enabled journalistic sources to be identified; *Nagla v. Latvia*, 2013, §§ 78-102, concerning urgent searches at the home of a journalist involving the seizure of data storage devices containing her sources of information; *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, 2015, §§ 101-120, regarding the seizure on a large scale of computer files and emails at a law firm's offices; and *Görmüş and Others v. Turkey*, 2016, §§ 32-77, on the protection of a journalist's sources, State officials who had highlighted unsatisfactory practices in their workplace, in the context of the confidentiality of military matters); and
- *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 442-458, concerning the bulk interception of communications, allowing intelligence services to access a large volume of confidential journalistic material inadvertently as a "bycatch" of the bulk operation. The Court found a violation of Article 10 of the Convention.

3. Data protection and prohibition of discrimination (Article 14 of the Convention)

329. In *Sheffield and Horsham v. the United Kingdom* [GC], 1998 (§§ 51-61, 76-77), which concerned the issue whether the respondent State had an obligation to legally recognise the new gender identity of the two applicants, who had undergone male-to-female gender reassignment surgery, the Court held that there had been no violation of Article 8 taken alone or in conjunction with Article 14. In the Court's view, situations in which the applicants might have to disclose their personal data did not occur with a degree of frequency which could be said to impinge to a disproportionate extent on their right to respect for their private lives. The Court also observed that the respondent State had endeavoured to some extent to minimise intrusive enquiries as to the gender status of transgender persons by allowing them to be issued with driving licences, passports and other types of official documents in their new name and gender, and that the use of birth certificates as a means of identification was officially discouraged (ibid., § 59; *Cossey v. the United Kingdom*, 1990, §§ 36-42).

330. In a few cases in which it has examined issues closely linked to personal data protection under Article 8 or Article 9, the Court has found no separate issue under Article 14 (*Sinan Işık v. Turkey*, 2010, § 57, concerning the indication – whether obligatory or optional – of the applicant's religion on his identity card; *Avilkina and Others v. Russia*, 2013, § 61, on the disclosure of the medical records of several Jehovah's Witnesses who had refused to undergo blood transfusions; *Christine Goodwin v. the United Kingdom* [GC], 2002, §§ 92-93 and 108, and *I. v. the United Kingdom* [GC], 2006, §§ 72-73, 88, concerning the legal recognition of an individual's gender reassignment).

4. Data protection and right to peaceful enjoyment of possessions (Article 1 of Protocol No. 1)

331. The Court has addressed personal data protection and the right to the peaceful enjoyment of possessions in the context of searches and seizures.

332. In *Smirnov v. Russia*, 2007 (§§ 53-59), the Court held that the national authorities had not struck a "fair balance" between the demands of the general interest of the community and the requirements of the protection of the applicant's right to the peaceful enjoyment of his possessions. There had therefore been a violation of Article 1 of Protocol No. 1 on account of the search carried out at the home of the applicant, a lawyer, followed by the seizure, among other items, of his computer's central unit containing hard disks with his personal data. While the retention of physical evidence might be necessary in the interests of the proper administration of justice, the computer itself had not been an object, instrument or product of any criminal offence. Since the information stored on the hard disk, which was potentially valuable and instrumental for the investigation, had been examined by the investigator, printed out and included in the case file, there had been no reason for the continued retention of the central unit. Moreover, the computer was the applicant's work tool and was also used to store his clients' data.

333. In the case of *Kruglov and Others v. Russia*, 2020 (§§ 145-146), the police searches of the homes and offices of the applicants, lawyers by profession, and their clients, and the seizure of computers and hard disks containing personal information and documents covered by professional secrecy – which were not in themselves an object, instrument or product of any criminal offence – were found to be in breach of Article 1 of Protocol No. 1.

334. In *Pendov v. Bulgaria*, 2020 (§§ 43-51), the Court held that the unnecessarily prolonged retention of the applicant's computer server in the context of criminal proceedings against third parties amounted to a violation of Article 1 of Protocol No. 1. The fact that the server had never been examined for the purposes of the criminal investigation, which related solely to third parties; the possibility of copying the necessary information; the importance of the server for the applicant's professional activity; and the partial inactivity of the public prosecutor's office, all meant that the retention of the applicant's server for seven and a half months had been disproportionate (ibid., § 51).

5. Data protection and freedom of movement (Article 2 of Protocol No. 4)

335. The Court has dealt with a number of cases in which an individual's freedom of movement was restricted because of personal data stored by the authorities. The Court examined the cases under Article 8.

336. Hence, in the case of *Dalea v. France* (dec.), 2010, the storage by the police, in the Schengen Information System, of data whose accuracy was contested by the applicant prevented him from travelling freely within the Schengen area. The applicant was unable to gain access to the personal data contained in the database and to have it rectified. The Court reiterated that Article 8 did not as such guarantee the right of an alien to enter or to reside in a particular country. In the present case, the interference with the applicant's private life on account of his inclusion by the French authorities in the Schengen database had been in accordance with the law and had pursued the legitimate aim of

protecting national security. It had been proportionate to the aim pursued and had been necessary in a democratic society. The applicant did not rely on Article 2 of Protocol No. 4.

337. In *Shimovolos v. Russia*, 2011 (§§ 64-71), information on the applicant's journeys by train and airplane had been recorded in the "surveillance database" owing to his membership of a human-rights organisation. Whenever a person whose name was on that list purchased a train or airline ticket, the Interior Department of Transport received an automatic notification. As a result, when the applicant boarded a train to travel to Samara in connection with an EU-Russia summit and to take part in a protest rally in that city, three police officers had checked his identity papers and asked him the reason for his travel. The Court found that by gathering and storing data on the applicant's movements under a ministerial order that had not been published and was not accessible to the public, the authorities had interfered with his private life in a manner incompatible with the rights guaranteed by Article 8. The Court further found that no separate issue arose under Article 2 of Protocol No. 4 (ibid., § 73).

338. In the case of *Beghal v. the United Kingdom*, 2019 (§§ 89-109), which raised the issue of the importance of monitoring terrorists' international movements, the Court considered, before finding a violation of Article 8, that the powers conferred under counter-terrorism legislation on police, immigration officers and designated customs officers to stop, search and question passengers at ports, airports and international rail terminals were not sufficiently circumscribed, nor were there adequate legal safeguards against abuse. In particular, the legislation did not require prior authorisation and the power to stop and question could be exercised even where there was no suspicion of involvement in terrorism.

339. In the case of *Willems v. the Netherlands* (dec.), 2021, concerning the obligation under the Passport Act to have fingerprints taken when applying for a passport, as well as the storage of such prints on an electronic chip, following the incorporation into domestic law (with no latitude left to national authorities) of the EU Regulation on standards for security features and biometrics in passports and travel documents issued by Member States, the complaints were dismissed as manifestly ill-founded owing to the "presumption of equivalent protection" in EU law (ibid., §§ 26-36).

B. Data protection and procedural rights

Article 6 of the Convention

> "1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.
>
> 2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
>
> 3. Everyone charged with a criminal offence has the following minimum rights:
>
> (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
>
> (b) to have adequate time and facilities for the preparation of his defence;
>
> (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
>
> (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
>
> (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court."

Article 13 of the Convention

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

1. Right to a fair trial (Article 6 of the Convention)[12]

340. Any individual whose personal data undergo automatic processing in the context of judicial proceedings must enjoy the guarantees of Article 6, irrespective of his or her status in the proceedings (applicant, respondent, witness, accused or third party).

a. General guarantees (Article 6 § 1 of the Convention)

341. In several cases the Court has assessed from the standpoint of Article 6 § 1 the need to protect the personal data of the parties or third parties, in the context of the various general guarantees designed to ensure the fairness of judicial proceedings. These include, in particular, equality of arms and the right to adversarial proceedings, the right to a public hearing and public pronouncement of judgment, the taking of evidence, the reasonable length of proceedings and the requirement to give reasons for judicial decisions.

[12] This chapter should be read in the light of and in conjunction with the Guides on Article 6 under its civil limb (pp. 60-91) and its criminal limb (pp. 32-100).

i. Equality of arms and respect for the adversarial principle in proceedings involving sensitive or confidential information

342. In the case of *Eternit v. France* (dec.), 2012 (§§ 35-42), an employer brought proceedings contesting the health insurance office's decision to recognise the occupational nature of the illness of one of its employees. The Court did not find the proceedings to be in breach of Article 6 § 1 despite the fact that the employer had not been provided with a copy of the observations made by the insurance office's medical adviser. The failure to provide the employer with the employee's medical records was justified by the need to protect the confidentiality of his medical data, which the courts had to give equal ranking with the applicant company's right to adversarial proceedings, so as to ensure that the very essence of the right was not impaired in either case. The requisite balance was achieved where the employer could ask the court to appoint an independent medical expert to review the employee's medical records and draw up a report – respecting the confidentiality of the medical records – to guide the court and the parties (ibid., § 37). The fact that an expert report was not commissioned every time an employer requested one, but only when the court considered it had insufficient information, was not contrary to the requirements of a fair trial under Article 6 § 1 de la Convention (ibid., §§ 35-39).

343. In *Kennedy v. the United Kingdom*, 2010 (§§ 184-191), restrictions on the principle of equality of arms and the adversarial principle in proceedings before the Investigatory Powers Tribunal, an independent body set up to examine complaints by persons suspecting that their communications had been unlawfully intercepted by the authorities, were not considered incompatible with Article 6 § 1. The interests of national security and the need to keep certain criminal investigation methods secret had to be weighed against the right to adversarial proceedings. In the Court's view, there had been a need to keep secret sensitive and confidential material, the disclosure of which would have prevented the achievement of the aim pursued (ibid., §§ 186-187).

344. More generally, the Court has stressed that the right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party including, for instance, a video recording of an accused used in evidence against her (*Murtazaliyeva v. Russia*, [GC], 2018, §§ 90-95).

ii. Reasoning of judicial decisions and data protection

345. In the case of *Surikov v. Ukraine*, 2017 (§§ 102-103), the Court found a violation of Article 6 § 1 on the grounds that the national courts had not addressed a number of pertinent and important points that had been raised. The applicant alleged that his employer had arbitrarily collected and stored sensitive and outdated information concerning his mental health, had used the information in examining his application for promotion, and had unlawfully disclosed it to his colleagues and to the court. The Court reaffirmed that Article 6 obliged the courts to give reasons for their judgments. Although that obligation could not be understood as requiring a detailed answer to every argument, the principle of fairness would be disturbed if the domestic courts ignored a specific, pertinent and important point made by an applicant (ibid., § 101 and the case-law cited therein).

346. In the case of *Samoylova v. Russia*, 2021 (§§ 50-52), which concerned the broadcast of a television report showing the applicant's exact address, her tax identification number and pictures from inside her country house, the Court found that the domestic courts had failed to provide a specific and explicit response to the arguments which would have been decisive for the outcome of the proceedings brought by the applicant, in disregard of the right to a fair hearing guaranteed by Article 6 § 1 by the Convention.

347. In the case of *Kennedy v. the United Kingdom*, 2010 (§§ 185-191), the authorities' policy of "neither confirming nor denying" that a communications interception operation had been carried out was not held to be incompatible with Article 6 § 1. Hence, it had been sufficient for the Investigatory

Powers Tribunal, set up to examine complaints by persons suspecting that their communications had been unlawfully intercepted by the authorities, to simply inform the applicants that no determination had been made in their favour, as the "neither confirm nor deny" policy of the Government could be circumvented if an application to that tribunal resulted in a complainant being advised whether interception had taken place (ibid., § 189).

iii. Use in evidence of personal data collected unlawfully or in breach of Article 8

348. The issue of the use as physical evidence in judicial proceedings of personal data collected in a manner contrary to the requirements of domestic law or those of Article 8 has been addressed by the Court in several cases, in the context of administrative proceedings (*Vukota-Bojic v. Switzerland*, 2016, § 77, on the use in a dispute with an insured person of information collected secretly by an insurance company within the scope of its powers under the public insurance scheme); civil proceedings (*Bărbulescu v. Romania* [GC], 2017, §§ 140-141, on the use of data collected by an employer concerning an employee's use of Internet in the workplace, in order to justify his dismissal; *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 2022, §§ 130-140, on the use of GPS mileage data recorded on a medical representative's company vehicle as grounds for his dismissal); and criminal proceedings (*Bykov v. Russia* [GC], 2009, §§ 80-83, on the interception of a conversation as part of a covert police operation and the use of the evidence thus obtained as the basis for a conviction).

349. The Court has held that the admission and use in judicial proceedings of evidence of this nature will not automatically lead to a finding that the proceedings were unfair if those proceedings as a whole were conducted fairly (*Bykov v. Russia* [GC], 2009, §§ 89-91; *Vukota-Bojic v. Switzerland*, 2016, §§ 91-100).

350. The Court found a violation of Article 6 § 1 in a case concerning information obtained through a police informer using a covert device for recording conversations in the applicant's cell, a measure that was not "in accordance with the law" (*Allan v. the United Kingdom*, 2002, §§ 45-53). The applicant's admissions had not been spontaneous but had been induced by the persistent questioning of the informer who, at the instigation of the police, had channelled the conversations in circumstances which could be regarded as the functional equivalent of interrogation, without any of the safeguards which would attach to a formal police interview. While there had been no special relationship between the applicant and the informer and no direct coercion had been identified, the applicant would have been subject to psychological pressures which impinged on the voluntary nature of the admissions. In those circumstances, the information gained could be regarded as having been obtained in defiance of the applicant's will and its use at his trial as impinging on his right to remain silent and the privilege against self-incrimination.

iv. Public hearing and public pronouncement of judgment and confidentiality of data[13]

351. In the case of *P. and B. v. the United Kingdom*, 2001 (§§ 38-41, 46-49), the lack of a public hearing and the pronouncement of a judgment in chambers in a child residence case were found not to be contrary to Article 6 § 1. In the Court's view, child custody proceedings were prime examples of cases where the exclusion of the press and public might be justified in order to protect the personal data of the child concerned and of the parties and to avoid prejudicing the interests of justice (ibid., § 38). The fact that anyone who could establish an interest could consult or obtain a copy of the full text of the orders and judgments, and that the courts' judgments were routinely published without giving the names of the persons concerned, was sufficient to compensate for the absence of public pronouncement (ibid., § 47).

[13] See also, above, the section of the present Guide on the Disclosure of data in the context of judicial proceedings from the standpoint of Article 8 of the Convention.

352. In *Kennedy v. the United Kingdom*, 2010 (§ 188), the Court reiterated that under Article 6 § 1 national security might justify the exclusion of the public from the proceedings. It held that the nature of the issues raised before the Investigatory Powers Tribunal, which related to the unlawful interception of communications, justified the absence of a public hearing.

353. The Court found a double violation of Article 6 in the case of *Vasil Vasilev v. Bulgaria*, 2021, regarding the total lack of public access (exclusion of public from all hearings and no public pronouncement of judgment) in proceedings that the applicant had brought to obtain damages following the interception, recording and transcription of a telephone conversation between him and a client, who had been under covert surveillance in a criminal case. The exclusion of the public from all hearings and from the delivery of the judgment had been based solely on the presence of classified information in the file (evidence stemming from covert interception of the applicant's telephone conversation). In the Court's view, the total lack of public access could not be justified by the need to protect the classified information which was the subject matter of the case. The nature of the questions raised during the proceedings, which concerned the responsibility of the State authorities for an alleged violation of Article 8 rights was not of a highly technical nature and the applicant had not waived his right to a public hearing (ibid., §§ 107-111). When a case relates to an alleged infringement of a fundamental right by the State authorities, public scrutiny of the proceedings is essential for maintaining confidence in the rule of law. The presence of classified information in the case file cannot in itself be grounds to withhold the entire judgment from the public. If a case involves classified information, techniques exist to allow some degree of public access to the decisions given in it while maintaining the confidentiality of sensitive information (ibid., §§ 116-118).

v. Length of judicial proceedings concerning data protection

354. In the case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017 (§ 215), the Court held that the overall duration – six years and six months across two levels of jurisdiction – of proceedings concerning the compatibility with domestic and European Union law of the mass publication of personal taxation data by the applicant companies did not satisfy the reasonable-time requirement under Article 6 § 1. The proceedings before the Court of Justice of the European Union concerning a request for a preliminary ruling could not be taken into consideration in assessing the length attributable to the domestic authorities (ibid., § 208).

355. By contrast, in the case of *Surikov v. Ukraine*, 2017 (§§ 104-106), the Court declared manifestly ill-founded a complaint regarding the length of proceedings relating to the storage by an employer of sensitive and outdated information on the mental health of an employee and its use in examining his application for promotion. The Court found that a period of less than six years over three levels of jurisdiction did not raise an issue with regard to the reasonable-time requirement under Article 6 § 1 (ibid., § 101).

b. Specific guarantees (Article 6 §§ 2 and 3 of the Convention)

356. In criminal matters, any individual who faces charges based on his or her personal data must be afforded certain specific guarantees.

i. Data protection and the right to be presumed innocent (Article 6 § 2 of the Convention)

357. In the case of *Batiashvili v. Georgia*, 2019 (§§ 87-97), the Court found Article 6 § 2 to be applicable in a situation where the authorities had manipulated a recording of an individual's telephone conversations prior to his arrest and had it broadcast on television. In the Court's view, the authorities' involvement had contributed to the applicant being perceived as guilty before his guilt was proved in court, and therefore amounted to a violation of Article 6 § 2. The sequence of events, considered as a whole, indicated that the applicant's situation had been substantially affected by the conduct of the investigating authorities (ibid., § 94). While the charge of failing to report a crime had

been dropped in the course of the first-instance proceedings, the indictment sent for trial almost four months after the recording was made available to the public had still referred to the charge in question, even though the prosecuting authorities must have been well aware of the falseness of the evidence underlying that charge (ibid., § 95).

358. In *Y.B. and Others v. Turkey*, 2004 (§§ 43-51), statements made to the press by the police with regard to suspects who were photographed by journalists at a press conference held on police premises were found to be in breach of Article 6 § 2. The publication of photographs of suspects in the course of criminal proceedings did not in itself amount to a breach of their right to be presumed innocent. The national authorities were entitled to inform the public about ongoing criminal investigations, provided this was done with all the discretion and prudence required. Nevertheless, where they made public objective information concerning criminal proceedings, this information had to be free from any assessment or prejudging of guilt (ibid., §§ 47-48). In the instant case the attitude of the police authorities, in so far as it entailed a prior assessment of the charges which the applicants might face and provided the press with an easy physical means of identifying them, was incompatible with the presumption of innocence (ibid., § 50).

359. In the case of *Panteleyenko v. Ukraine,* 2006 (§ 68-71), the court decisions terminating the criminal proceedings against the applicant were couched in terms which left no doubt as to the judges' view that the applicant had committed the offence with which he was charged; the Court therefore found a violation of Article 6 § 2. The decision discontinuing the proceedings on "non-exonerative grounds" had been taken on the basis of evidence containing personal data pertaining to the applicant, a notary by profession, and obtained following a search of his office conducted in breach of the statutory requirement to serve the search warrant in advance on a person occupying the relevant premises and of the prohibition on seizing any documents and items which did not directly relate to the case under investigation (ibid., § 70)[14].

ii. Data protection and defence rights (Article 6 § 3 (b) of the Convention)

360. In the case of *Rook v. Germany*, 2019 (§ 69), the Court ruled that a period of three and a half months to study a large volume of data and electronic files on the applicant, obtained by telecommunication surveillance, was sufficient from the perspective of Article 6 § 3 (b) to enable his lawyer to prepare his defence. In view of the complexity of the criminal proceedings, it had not been necessary to give the applicant's lawyer an opportunity to read and listen to each and every item of surveillance data, comprising 45,000 telephone calls and 34,000 other data sets collected in the course of the investigation, and 14 million electronic files which the police had confiscated at the applicant's apartment and at other locations (ibid., §§ 7-8, 67-71).

361. More generally, the Court stressed that modern investigation methods might indeed produce enormous amounts of data, the integration of which into the criminal proceedings should not cause unnecessary delays to those proceedings. The applicant's right to disclosure was not to be confused with his right of access to all material already considered relevant by the authorities, which generally required that the person concerned should be able to comprehend the material in its entirety (ibid., § 67). The mere fact that the court proceedings had already begun when the lawyer obtained a full copy of the file did not mean that he had not had sufficient time to prepare. Article 6 § 3 (b) does not require the preparation of a trial lasting over a certain period of time to be completed before the first hearing (ibid., § 72)[15].

[14] See also the Guide on Article 6 of the Convention (Right to a fair trial (criminal limb)) with regard to the reasoning of judicial decisions (paragraphs 168-176)

[15] See also the Guide on Article 6 of the Convention (Right to a fair trial (criminal limb)) with regard to the facilities required by accused persons for the preparation of their defence.

362. In the case of *Sigurður Einarsson and Others v. Iceland*, 2019 (§§ 88-93), the Court found that there had been no violation of Article 6 §§ 1 and 3 (b) concerning the defence's lack of access to the vast amount of data collected by the prosecution and not included in the investigation file, and the fact that the defence did not have a say in the prosecution's electronic sifting of that data in order to identify the information relevant to the investigation. With regard to the "full collection of data", the prosecution had not been aware of what the contents of the mass of data were, and to that extent it had not held any advantage over the defence. As to the "tagged" data, in principle it would have been appropriate for the defence to be afforded the possibility of conducting a search for potentially disculpatory evidence. However, the applicants had not at any stage formally sought a court order to that effect and had not specified the type of evidence they were seeking.

2. Right to an effective remedy (Article 13 of the Convention)[16]

363. In the case of *Anne-Marie Anderson v. Sweden*, 1997 (§§ 41-42), concerning the disclosure of medical records, the Court found no violation of Article 13 read in conjunction with Article 8 with regard to the lack of possibility for a patient, prior to the communication of personal and confidential medical data by the medical authority to a social services authority, to challenge the measure. Among other things, the measure had been notified to the applicant and had been of a limited nature as the information concerned had not been made public but had been protected by the same level of confidentiality as that applicable to psychiatric records.

364. In *Mik and Jovanović v. Serbia* (dec.) the applicants complained under Article 8 alone and in conjunction with Article 13 about the State's continuing failure to provide them with credible information about the fate of their infant sons who had allegedly died shortly after their birth and whose bodies had never been shown to the applicants, the Court noted that a recently adopted legislative act had established a mechanism (including DNA database) with respect to the situation faced by the applicants and others. In particular, the new legal framework provided for both judicial and extrajudicial procedures aimed at discovering the true status of newborn children suspected to have disappeared from State maternity wards and providing redress to parents. Moreover, certain important steps had been taken to implement that framework, including extensive training of judges as well as the appointment, in the context of extrajudicial procedure, of members (representatives of registered parents' associations being their majority) of a commission with extensive investigatory, data collection and reporting powers. Noting that the applicants themselves had opted in favour of making use of the new mechanism, the Court concluded that it was no longer justified to continue the examination of the application within the meaning of Article 37 § 1 (c) of the Convention.

365. In *Panteleyenko v. Ukraine*, 2006 (§§ 82-84), the Court found a violation of Article 13 taken together with Article 8 in view of the absence of an effective remedy enabling the applicant to complain about the disclosure of confidential information about his mental health at a public hearing. In the Court's view, the existing legal remedies had proved ineffective because they had not resulted in the discontinuation of the disclosure of confidential psychiatric data in the court case file or any award to the applicant of compensation for the damage suffered as the result of the interference with his private life. Although a hearing in camera would have prevented the information from being disclosed to the public, it would not have prevented it from coming to the knowledge of the parties or being included in the case file.

366. Regarding the posting on the Internet of a judicial decision disclosing information concerning the adoption of the applicants' children, the Court held, in the case of *X and Others v. Russia*, 2020 (§§ 73-79), that there had been a violation of Article 13 taken together with Article 8 owing to the lack of a

[16] This chapter should be read in the light of and in conjunction with the Guide on Article 13 of the Convention (Right to an effective remedy, see, in particular, pages 49-51).

judicial remedy affording compensation for the non-pecuniary damage caused by the malfunctioning of the justice system.

367. In a case concerning the entry of an individual as an "offender" in the police registers after he was questioned in connection with a rape, and the retention of the entry although no bill of indictment was filed subsequently, the Court found a violation of Article 13 read in conjunction with Article 8 after observing that the applicant had not had any remedy at the relevant time by which to complain of the measure (*Dimitrov-Kazakov v. Bulgaria*, 2011, §§ 37-39).

368. The lack of an effective remedy enabling the applicant to request the removal of his name from the list annexed to the Taliban Ordinance amounted to a violation of Article 13 taken together with Article 8 in *Nada v. Switzerland* [GC], 2012 (§§ 209-214). The applicant had been able to apply to the domestic courts but they had not examined his complaints on the merits.

369. Regarding the use of personal data in a professional context, the Court found a violation of Article 13 taken together with Article 8 in *Smith and Grady v. the United Kingdom*, 1999 (§§ 136-139), on account of the lack of an effective remedy in respect of the breach of the applicants' privacy as a result of intrusive investigations into the private lives of homosexuals leading to their discharge from the armed forces.

370. In the case of *Karabeyoğlu v. Turkey*, 2016 (§§ 128-132), the unavailability of a domestic remedy by which to secure a review of the use in disciplinary proceedings of data obtained by telephone tapping in a criminal investigation led the Court to find a violation of Article 13 read in the light of Article 8.

371. In *Peck v. the United Kingdom*, 2003 (§§ 101-114), the Court ruled that the applicant had not had any effective remedy by which to complain of the disclosure to the media of CCTV footage showing him attempting to commit suicide in a public place. With regard to the possibility of judicial review, since the sole issue before the domestic courts had been whether the policy regarding images captured by CCTV cameras in public places could be said to be "irrational", any consideration of the question whether the interference with the applicant's right answered a pressing social need or was proportionate was effectively excluded (ibid., §§ 106-107). As to the media commissions, their lack of power to award damages meant that they could not provide an effective remedy either (ibid., §§ 108-109). As to an action in breach of confidence, it was unlikely that the courts would have accepted at the relevant time that the images had the "necessary quality of confidence" or that the information had been "imparted in circumstances importing an obligation of confidence" (ibid., § 111).

372. On the subject of secret surveillance, the secrecy of measures makes it difficult, if not impossible, for the person concerned to exercise a remedy, particularly while the surveillance is in progress. An "effective remedy" for the purposes of Article 13 must mean a remedy that is as effective as it can be having regard to the restricted scope for recourse inherent in any system of surveillance (*Klass and Others v. Germany*, 1978, §§ 68-69). Objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must be made available to the individual concerned, within a reasonable time (*Rotaru v. Romania* [GC], 2000, § 69).

373. As regards targeted secret surveillance measures, where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure. After the surveillance measure has been lifted the persons concerned should be provided with information as soon as notification can be carried out without jeopardising the purpose of the restriction. To enable the person concerned to obtain a review of the proceedings concerning the interference with the exercise of his or her right to private life, it is in principle necessary to provide that individual with a minimum amount of information on the

decision that could be challenged, such as its date of adoption and the court which has issued it (*Roman Zakharov v. Russia* [GC], 2015, §§ 233, 287, 294; *İrfan Güzel v. Turkey*, 2017, §§ 96, 98-99).

374. In the case of *Klass and Others v. Germany*, 1978 (§§ 65-72), the "G10" Act allowed the authorities to open and inspect mail and post, read telegraphic messages, and listen to and record telephone conversations, in order to defend the country against "imminent dangers". The Court held that the aggregate of remedies provided for under German law satisfied, in the particular circumstances of that case, the requirements of Article 13 in the light of Article 8 concerning respect for private life and correspondence. Even though, according to the Act, the ordering and implementation of the restrictive measures could not be challenged in the courts, various other remedies were available to individuals who believed themselves to be under surveillance. According to the 1970 judgment of the Federal Constitutional Court, the competent authority was required to inform the person concerned as soon as the surveillance measures were discontinued, and notification could be made without jeopardising the purpose of the restriction. From the moment of such notification, various legal remedies before the courts became available to individuals. They could: bring an action for a declaration in order to obtain a review by the administrative courts as to whether the G10 had been applied lawfully in their case and whether the surveillance measures ordered were in conformity with the law; institute an action for damages in a civil court if they had been prejudiced; or bring an action for the destruction or, if appropriate, restitution of documents. Finally, if none of those remedies was successful, they could apply to the Federal Constitutional Court for a ruling as to whether there had been a breach of the Basic Law. See also, to similar effect, the cases of *Leander v. Sweden*, 1987 (§§ 78-84), concerning a system of secret checks on candidates for employment in posts of importance from a national security perspective, and *Amann v. Switzerland* [GC], 2000 (§§ 89-90), relating to the interception and recording of a telephone call and the storage of personal data by the intelligence services.

375. In view of the failure to respond to the misgivings of an accused as to the lawfulness of the tapping of his telephone calls, the Court found a violation of Article 13 taken together with Article 8 in the case of *İrfan Güzel v. Turkey*, 2017 (§§ 100-109).

376. In *Allan v. the United Kingdom*, 2002 (§ 55), the Court found a violation of Article 13 read in conjunction with Article 8 on the grounds that no statutory system had existed at the relevant time regulating the use of covert devices to record conversations in the applicant's cell and their use by the police.

377. In a case where overall control over a covert surveillance system was entrusted solely to the Minister of Internal Affairs (which was directly involved in requests for the use of special surveillance means to protect national security), rather than to independent bodies, the Court found a violation of Article 13 in the light of Article 8 owing to the lack of an effective remedy (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 2007, §§ 98-103).

378. In view of the lack of a remedy by which to challenge the storage by State agents of data concerning an individual's private life or the veracity of that information, the Court found a violation of Article 13 read in conjunction with Article 8 in the case of *Rotaru v. Romania* [GC], 2000 (§§ 68-73). It reached a similar finding in *Segerstedt-Wiberg and Others v. Sweden*, 2006 (§§ 116-122), in the absence of a remedy allowing the applicants to view in its entirety the information about them in the security police files and to obtain the destruction of the files kept on them by the security police and the erasure or rectification of the personal information in those files.

3. Right to liberty and security (Article 5 of the Convention)

379. In the case of *Akgün v. Turkey*, 2021 (§§ 178-181), where at the time of the applicant's initial pre-trial detention the finding that he had used the encrypted ByLock messaging system was the only evidence which was provided to justify the suspicion, for the purposes of Article 5 § 1 (c), that he had committed the offence of belonging to a terrorist organisation, the Court found a violation of that

Convention provision. The applicant's alleged criminal activity concerned organised crime. The use of electronic evidence indicating that an individual availed himself of an encrypted messaging service which had been specially designed for and exclusively used by a criminal organisation for the purposes of that organisation's internal communication could be a significant instrument in combatting organised crime. In consequence, a suspect could validly be detained at the outset of proceedings on the basis of such evidence, as it could provide a strong indication that that individual belonged to such an organisation. Where such evidence formed the sole or exclusive basis of the suspicions against an individual, the national court had to have available sufficient information about the material in question before examining, with prudence, its possible evidential value under domestic law. In this case the Government had been unable to show that at the date on which the applicant was placed in pre-trial detention the evidence available to the magistrate's court had met the standard of "reasonable suspicion" that was required by Article 5 § 1 (c) of the Convention, such as to satisfy an objective observer that he might have committed the offences for which he had been detained. In the Court's view, the document concluding that the applicant had used ByLock did not as such specify or set out any illegal activity on the applicant's part, in that it did not identify either the dates of this presumed activity or its frequency, and did not contain any additional related details. Furthermore, neither this document nor the pre-trial detention order had how this presumed activity by the applicant indicated his membership of a terrorist organisation.

IV. Modern-day challenges of data protection

A. Technological advances, algorithms and artificial intelligence[17]

380. In cases concerning the taking and storage by the authorities, for crime-prevention purposes, of fingerprints, biological samples and DNA profiles of persons suspected or convicted of offences, the Court has stated clearly that the use of modern scientific techniques cannot be authorised at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests (*S. and Marper v. the United Kingdom* [GC], 2008, § 112). Any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard (ibid., § 112). Bearing in mind the rapid pace of developments in the field of genetics and information technology, the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today cannot be discounted (ibid., § 71).

381. In the Court's view, the rapid development of increasingly sophisticated techniques allowing, among other things, facial recognition and facial mapping techniques to be applied to individuals' photographs, makes the taking of their photographs and the storage and possible dissemination of the resulting data problematic. The domestic courts must take account of these factors in assessing the necessity of the interference with the private life of the person concerned (*Gaughran v. the United Kingdom*, 2020, § 70). In that case (ibid., §§ 96-98), the Court stressed that modern technology was more complex and that the domestic courts had not given sufficient consideration to this aspect in examining the necessity of the interference with the right to respect for private life of the applicant, whose photograph had been taken by the authorities following a minor offence and had been retained even after his conviction had been erased from the records on expiry of the statutory period.

382. In *Breyer v. Germany*, 2020 (§ 88), the Court recognised, in the context of the fight against organised crime and terrorism, that modern means of telecommunications and changes in

[17] This chapter should be read in conjunction with the sections of the present Guide on Storage of personal data for the purposes of combating crime and Data collection by the authorities via covert surveillance.

communication behaviour required that investigative tools be adapted. In the Court's view, the obligation for mobile-telephone operators to store subscriber information and make it available to the authorities on request is, in general, a suitable response to changes in communication behaviour and in the means of telecommunications.

383. In *Szabó and Vissy v. Hungary*, 2016 (§ 68), a case concerning mass surveillance of communications, the Court acknowledged that it was a natural consequence of the forms taken by present-day terrorism that governments would resort to cutting-edge technologies, including the massive monitoring of communications, in order to pre-empt imminent attacks. In this case the Court held that the legislation allowing mass surveillance did not provide the necessary safeguards against abuse, because new technologies made it easy for the authorities to intercept large quantities of data relating even to people not in the category originally targeted by the operation. Moreover, measures of this kind could be ordered by the executive without any control and without any assessment as to whether they were strictly necessary, and in the absence of any effective judicial or other remedy (ibid., §§ 73-89).

384. In the case of *Roman Zakharov v. Russia* [GC], 2015 (§§ 302-305), the Court held that the risk of abuse inherent in any system of secret surveillance was particularly high in a system where the secret services and the police had direct access, by technical means, to all mobile-telephone communications. The Court found a violation of Article 8, taking the view that the Russian legal provisions allowing generalised interception of communications did not provide adequate and effective guarantees against arbitrariness and the risk of abuse inherent in any system of secret surveillance.

385. In the case of *Akgün v. Turkey*, 2021 (§§ 178-181), where at the time of the applicant's initial pre-trial detention the finding that he had used the encrypted ByLock messaging system was the only evidence which was provided to justify the suspicion, for the purposes of Article 5 § 1 (c), that he had committed an offence, the Court emphasised that the use of such evidence as the sole basis underlying a suspicion could pose a number of delicate issues, since, by their nature, the procedure and technologies applied in gathering this evidence were complex and could accordingly reduce the ability of the national courts to establish their authenticity, accuracy and integrity (see paragraph 373 above).

386. In the cases *Centrum för rättvisa v. Sweden* [GC], 2021, § 261, and *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 322-323, the Court expressly admitted that the use of a bulk interception regime was not *per se* contrary to Article 8, in view of the proliferation of threats that States currently faced from networks of international actors, using the Internet for communication, and the existence of sophisticated technology which enabled these actors to avoid detection. The Court nevertheless emphasised that in view of the constant development in modern communication technologies, its usual approach to targeted surveillance regimes would have to be adapted to reflect the specific features of a bulk interception regime, on account of the risk of the bulk interception power being abused and of the legitimate need for secrecy in such operations. In particular the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review.

B. Internet and search engines

387. Internet sites are an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information (*M.L. and W.W. v. Germany*, 2018, § 91). 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 generally (*Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2),* 2009, § 27).

388. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press, particularly on account of the important role of search engines (*M.L. and W.W. v. Germany*, 2018, § 91 and the references cited therein).

389. Information containing personal data held by media outlets can easily be found by Internet users via search engines (ibid., § 97). Because of this amplifying effect on the dissemination of information and the nature of the activity underlying the publication of information, the obligations of search engines towards the individual who is the subject of the information may differ from those of the entity which originally published the information (ibid., § 97). Hence, in a case in which two individuals had requested that the full details of their identity and their photographs be removed from the online archives of certain newspapers and radio stations after they had finished serving long prison sentences for murder (ibid., §§ 7, 12, 33), the Court found that the balancing of the interests at stake could result in different outcomes depending on whether a request for the deletion of personal data concerned the original publisher of the information, whose activity was generally at the heart of what freedom of expression was intended to protect, or a search engine whose main interest was not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her (ibid., § 97). See also paragraphs 281 and 282 above of the present Guide for more information on the "right to be forgotten" in the context of the online archives of media outlets containing individuals' personal data, in the case of *M.L. and W.W. v. Germany*.

390. In the Court's view, Internet archives contribute to preserving and making available news and information (*Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2),* 2009, § 45). Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free.

391. The discretion afforded to States in striking a balance between the competing rights is greater where news archives of past events, rather than news reporting of current affairs, are concerned (ibid., § 45). The duty of the press to act in accordance with the principles of responsible journalism by ensuring the accuracy of historical, rather than perishable, information published is more stringent in the absence of any urgency in publishing the material (ibid., § 45).

392. The refusal of the courts to order the withdrawal of an article damaging the reputation of a lawyer and available in a newspaper's Internet archives was found not to be in breach of Article 8 in the case of *Węgrzynowski and Smolczewski v. Poland*, 2013 (§§ 60-70). The Court accepted that it was not the role of the judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which had in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations (ibid., § 65). Furthermore, the legitimate interest of the public in access to the public Internet archives of the press was protected under Article 10 (ibid., § 65). It was noteworthy that the Polish courts had observed that it would be desirable to add a comment to the article on the newspaper's website informing the public of the outcome of the first set of proceedings. In the Court's view, this showed that the domestic courts had been aware of the significance which publications available to the general public on the Internet could have for the effective protection of individual rights and that they appreciated the value of the availability on the newspaper's website of full information about the judicial decisions concerning the article. The lawyer had not requested that a reference to the earlier judgments in his favour be added to the article (ibid., §§ 66-67).

393. The case of *Biancardi v. Italy*, 2021, §§ 67-70, afforded the Court its first opportunity to rule on the compatibility with Article 10 of a civil judgment against a journalist for not de-indexing sensitive information published on the Internet concerning criminal proceedings against private individuals and

the journalist's decision to keep the information easily accessible in spite of opposition from those concerned. The question of anonymising identities in the on-line article did not arise in this case. The Court noted that the article had remained easily accessible online for eight months after a formal request to remove it by the persons concerned. The severity of the sanction – liability under civil and not criminal law – and the amount of the compensation awarded did not appear excessive.

C. Data transfers and data flows

394. In *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, a case concerning mass flows of personal data, personal taxation data on 1.2 million individuals were published in a magazine and subsequently disseminated by means of a text messaging service. In the Court's view, the existence of a public interest in providing access to, and allowing the collection of, large amounts of taxation data for journalistic purposes did not necessarily or automatically mean that there was also a public interest in disseminating *en masse* such raw data in unaltered form without any analytical input. A distinction had to be made between the processing of data for journalistic purposes and the dissemination of the raw data to which the journalists were given privileged access (ibid., § 175). In that context, the fact of prohibiting the mass publication of personal taxation data in a manner incompatible with Finnish and EU rules on data protection was not, as such, a sanction, despite the fact that, in practice, the limitations imposed on the quantity of the information to be published may have rendered some of the applicant companies' business activities less profitable (ibid., § 197).

395. The case of *Big Brother Watch and Others v. the United Kingdom* [GC], 2021 raised, *inter alia*, the question of the compatibility with Article 8 of the Convention of the sharing of data intercepted by foreign intelligence services, in this case the US National Security Agency ("NSA"). The Court stated that the exchange of data had to be framed by clear detailed rules which gave citizens an adequate indication of the circumstances in which and the conditions on which the authorities were empowered to make such requests and which provided effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention. Upon receipt of the intercept material, the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards were equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If States did not always know whether material received from foreign intelligence services was the product of interception, then the Court considered that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept. Finally, any regime permitting intelligence services to request either interception or intercept material from non-Contracting States should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review (ibid., §§ 498-499).

List of cited cases

The case-law cited in this Guide refers to judgments or decisions delivered by the Court and to decisions or reports of the European Commission of Human Rights ("the Commission").

Unless otherwise indicated, all references are to a judgment on the merits delivered by a Chamber of the Court. The abbreviation "(dec.)" indicates that the citation is of a decision of the Court and "[GC]" that the case was heard by the Grand Chamber.

Chamber judgments that are not final within the meaning of Article 44 of the Convention are marked with an asterisk in the list below. Article 44 § 2 of the Convention provides: "The judgment of a Chamber shall become final (a) when the parties declare that they will not request that the case be referred to the Grand Chamber; or (b) three months after the date of the judgment, if reference of the case to the Grand Chamber has not been requested; or (c) when the panel of the Grand Chamber rejects the request to refer under Article 43". In cases where a request for referral is accepted by the Grand Chamber panel, the Chamber judgment does not become final and thus has no legal effect; it is the subsequent Grand Chamber judgment that becomes final.

The hyperlinks to the cases cited in the electronic version of the Guide are directed to the HUDOC database (http://hudoc.echr.coe.int) which provides access to the case-law of the Court (Grand Chamber, Chamber and Committee judgments and decisions, communicated cases, advisory opinions and legal summaries from the Case-Law Information Note), and of the Commission (decisions and reports) and to the resolutions of the Committee of Ministers.

The Court delivers its judgments and decisions in English and/or French, its two official languages. HUDOC also contains translations of many important cases into more than thirty non-official languages, and links to around one hundred online case-law collections produced by third parties. All the language versions available for cited cases are accessible via the 'Language versions' tab in the HUDOC database, a tab which can be found after you click on the case hyperlink.

—A—

A.B. v. the Netherlands, no. 37328/97, 29 January 2002
A.P., Garçon and Nicot v. France, nos. 79885/12 and 2 others, ECHR 2017
Adomaitis v. Lithuania, no. 14833/18, 18 January 2022
Akgün v. Turkey, no. 19699/18, 20 July 2021
Allan v. the United Kingdom, no. 48539/99, ECHR 2002-IX
Alexandridis v. Greece, no. 19516/06, 21 February 2008
Alkaya v. Turkey, no. 42811/06, 9 October 2012
Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece, no. 72562/10, 22 February 2018
Amann v. Switzerland [GC], no. 27798/95, ECHR 2000-II
Anchev v. Bulgaria (dec.), nos. 38334/08 and 68242/16, 5 December 2017
André and Others v. France, no. 18603/03, 24 July 2008
Antoneta Tudor v. Romania, no. 23445/04, 24 September 2013
Antović and Mirković v. Montenegro, no. 70838/13, 28 November 2017
Apostu v. Romania, no. 22765/12, 3 February 2015
Armonienė v. Lithuania, no. 36919/02, 25 November 2008
Association « 21 December 1989 » and Others v. Romania, nos. 33810/07 and 18817/08, 24 May 2011

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, 28 June 2007
Avilkina and Others v. Russia, no. 1585/09, 6 June 2013
Axel Springer AG v. Germany [GC], no. 39954/08, 7 February 2012
Axel Springer SE and RTL Television GmbH v. Germany, no. 51405/12, 21 September 2017
Aycaguer v. France, no. 8806/12, 22 June 2017

—B—

B.B. v. France, no. 5335/06, 17 December 2009
Batiashvili v. Georgia, no. 8284/07, 10 October 2019
Bărbulescu v. Romania [GC], no. 61496/08, 5 September 2017 (extracts)
Bédat v. Switzerland [GC], no. 56925/08, ECHR 2016
Beghal v. the United Kingdom, no. 4755/16, 28 February 2019
Benedik v. Slovenia, no. 62357/14, 24 April 2018
Ben Faiza v. France, no. 31446/12, 8 February 2018
Bernh Larsen Holding AS and Others v. Norway, no. 24117/08, 14 March 2013
Biancardi v. Italy, no. 77419/16, 25 November 2021
Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, 25 May 2021
Biriuk v. Lithuania, no. 23373/03, 25 November 2008
Bogomolova v. Russia, no. 13812/09, 20 June 2017
Boljević v. Serbia, no. 47443/14, 16 June 2020
Brunet v. France, no. 21010/10, 18 September 2014
Breyer v. Germany, no. 50001/12, 30 January 2020
Buck v. Germany, no. 41604/98, ECHR 2005-IV
Buturugă v. Romania, no. 56867/15, 11 February 2020
Bykov v. Russia [GC], no. 4378/02, 10 March 2009

—C—

C.C. v. Spain, no. 1425/06, 6 October 2009
Cakicisoy and Others v. Cyprus (dec.), no. 6523/12, 23 September 2014
Canonne v. France (dec.), no. 22037/13, 2 June 2015
Caruana v. Malta (dec.), no. 41079/16, 15 May 2018
Catt v. the United Kingdom, no. 43514/15, 24 January 2019
Cemalettin Canlı v. Turkey, no. 22427/04, 18 November 2008
Centre for Democracy and the Rule of Law v. Ukraine v. Ukraine, no. 10090/16, 26 March 2020
Centrum för rättvisa v. Sweden [GC], no. 35252/08, 25 May 2021
Cevat Özel v. Turkey, no. 19602/06, 7 June 2016
Christine Goodwin v. the United Kingdom [GC], no. 28957/95, ECHR 2002-VI
Ciubotaru v. Moldova, no. 27138/04, 27 April 2010
Coban v. Spain (dec.), no. 17060/02, 25 September 2006
Copland v. the United Kingdom, no. 62617/00, ECHR 2007-I
Cossey v. the United Kingdom, 27 September 1990, Series A no. 184
Craxi v. Italy (no. 2), no. 25337/94, 17 July 2003

—D—

D.L. v. Bulgaria, no. 7472/14, 19 May 2006

Dalea v. France (dec.), no. 964/07, 2 February 2010
DELTA PEKÁRNY a.s. v. Czech Republic, no. 97/11, 2 October 2014
Demirtepe v. France, no. 34821/97, ECHR 1999-IX (extracts)
Deveci v. Türkiye (dec.), no. 42785/11, 28 June 2022
Dimitras and Others v. Greece, nos. 42837/06 and 4 others, 3 June 2010
Dimitrov-Kazakov v. Bulgaria, no. 11379/03, 10 February 2011
Doerga v. the Netherlands, no. 50210/99, 27 April 2004
Dragan Petrović v. Serbia, no. 75229/10, 14 April 2020
Dragojević v. Croatia, no. 68955/11, 15 January 2015
Drakšas v. Lithuania, no. 36662/04, 31 July 2012
Drelon v. France, nos. 3153/16 and 27758/18, 8 September 2022
Dudgeon v. the United Kingdom, 22 October 1981, Series A no. 45
Dumitru Popescu v. Romania (no. 2), no. 71525/01, 26 April 2007
Dupuis and Others v. France, no. 1914/02, 7 June 2007

—E—

Editions Plon v. France, no. 58148/00, ECHR 2004-IV
Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, ECHR 2011 (extracts)
Egeland and Hanseid v. Norway, no. 34438/04, 16 April 2009
Ekimdzhiev and Others v. Bulgaria, no. 70078/12, 11 January 2022
Elberte v. Latvia, no. 61243/08, ECHR 2015
Erdem v. Germany, no. 38321/97, ECHR 2001-VII (extracts)
Ernst and Others v. Belgium, no. 33400/96, 15 July 2003
Eternit v. France (dec.), no. 20041/10, 27 March 2012

—F—

Financial Times Ltd and Others v. the United Kingdom, no. 821/03, 15 December 2009
Florindo de Almeida Vasconcelos Gramaxo v. Portugal, no. 26968/16, 13 December 2022
Foxley v. the United Kingdom, no. 33274/96, 20 June 2000
Frâncu v. Romania, no. 69356/13, 13 October 2020
Friedl v. Austria, no. 15225/89, Commission report, 19 May 1994

—G—

G.S.B. v. Switzerland, no. 28601/11, 22 December 2015
Gafiuc v. Romania, no. 59174/13, 13 October 2020
Gardel v. France, no. 16428/05, ECHR 2009
Garnaga v. Ukraine, no. 20390/07, 16 May 2013
Gaskin v. the United Kingdom, 7 July 1989, Series A no. 160
Gaughran v. the United Kingdom, no. 45245/15, 13 February 2020
Gawlik v. Liechtenstein, no. 23922/19, 16 February 2021
Giesbert and Others v. France, nos. 68974/11 and 2 others, 1er June 2017
Gillan and Quinton v. the United Kingdom, no. 4158/05, ECHR 2010 (extracts)
Gîrleanu v. Romania, no. 50376/09, 26 June 2018
Godelli v. Italy, no. 33783/09, 25 September 2012
Gorlov and Others v. Russia, nos. 27057/06 and 2 others, 2 July 2019
Görmüş and Others v. Turkey, no. 49085/07, 19 January 2016

Grant v. the United Kingdom, no. 32570/03, ECHR 2006-VII
Greuter v. the Netherlands (dec.), no. 40045/98, 19 March 2002
Guerra and Others v. Italy, no. 14967/89, *Reports of Judgments and Decisions* 1998-I
Guillot v. France, 24 October 1996, *Reports of Judgments and Decisions* 1996-V
Guiorgui Nikolaïchvili v. Georgia, no. 37048/04, 13 January 2009
Güzel Erdagöz v. Turkey, no. 37483/02, 21 October 2008

—H—

Haldimann and Others v. Switzerland, no. 21830/09, ECHR 2015
Halford v. the United Kingdom, 25 June 1997, *Reports of Judgments and Decisions* 1997-III
Hämäläinen v. Finland [GC], no. 37359/09, ECHR 2014
Haralambie v. Romania, no. 21737/03, 27 October 2009
Hájovský v. Slovakia, no. 7796/16, 1 July 2021
Haščák v. Slovakia, nos. 58359/12 and 2 others, 23 June 2022
Hassine v. Romania, no. 36328/13, 9 March 2021
Heglas v. Czech Republic, no. 5935/02, 1 March 2007
Henry Kismoun v. France, no. 32265/10, 5 December 2013
Huvig v. France, 24 April 1990, Series A no. 176-B

—I—

I. v. Finland, no. 20511/03, 17 July 2008
I. v. the United Kingdom [GC], no. 25680/94, 11 July 2006
Iordachi and Others v. the Republic of Moldova, no. 25198/02, 10 February 2009
İrfan Güzel v. Turkey, no. 35285/08, 7 February 2017
Ivashchenko v. Russia, no. 61064/10, 13 February 2018

—J—

J.L. v. Italy, no. 5671/16, 27 May 2021
J.P.D. v. France (dec.), no. 55432/10, 16 September 2016
J.S. v. the United Kingdom (dec.), 445/10, 3 March2015
Jäggi v. Switzerland, no. 58757/00, ECHR 2006-X
Jarnea v. Romania, no. 41838/05, 19 July 2011
Jecker v. Switzerland, no. 35449/14, 6 October 2020
Joanna Szulc v. Poland, no. 43932/08, § 13 November 2012

—K—

K.H. and Others v. Slovakia, no. 32881/04, ECHR 2009 (extracts)
K.S. and M.S. v. Germany, no. 33696/11, 6 October 2016
K.U. v. Finland, no. 2872/02, ECHR 2008
Kahn v. Germany, no. 16313/10, 17 March 2016
Karabeyoğlu v. Turkey, no. 30083/10, 7 June 2016
Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010
Khadija Ismayilova v. Azerbaijan, nos. 65286/13 and 57270/14, 10 January 2019
Khan v. the United Kingdom, no. 35394/97, ECHR 2000-V

Khoujine and Others v. Russia, no. 13470/02, 23 October 2008
Khelili v. Switzerland, no. 16188/07, 18 October 2011
Kinnunen v. Finland, no. 18291/91, Commission decision, 13 October 1993
Kinnunen v. Finland, no. 24950/94, Commission decision, 15 May 1996
Kırdök and Others v. Turkey, no. 14704/12, 3 December 2019
Kiyutin v. Russia, no. 2700/10, ECHR 2011
Klass and Others v. Germany, 6 September 1978, Series A no. 28
Khmel v. Russia, no. 20383/04, 12 December 2013
Konovalova v. Russia, no. 37873/04, 9 October 2014
Köpke v. Germany (dec.), no. 420/07, 5 October 2010
Kotilainen and Others v. Finland, no. 62439/12, 17 September 2020
Krone Verlag GmbH & Co. KG v. Austria, no. 34315/96, 26 February 2002
Kruglov and Others v. Russia, nos. 11264/04 and 15 others, 4 February 2020
Kruslin v. France, 24 April 1990, Series A no. 176-A
Kurier Zeitungsverlag und Druckerei GmbH v. Austria, no. 3401/07, 17 January 2012
Kvasnica v. Slovakia, no. 72094/01, 9 June 2009

—L—

L.H. v. Latvia, no. 52019/07, 29 April 2014
L.L. v. France, no. 7508/02, ECHR 2006-XI
Labita v. Italy [GC], no. 26772/95, ECHR 2000-IV
Lambert v. France, no. 23618/94, *Reports of Judgments and Decisions* 1998-V
Lavents v. Latvia, no. 58442/00, 28 November 2002
Leander v. Sweden, 26 March 1987, Series A no. 116
Libert v. France, no. 588/13, 22 February 2018
Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008
Liblik and Others v. Estonia, no. 173/15 and 5 others, 28 May 2019
Liebscher v. Austria, no. 5434/17, 6 April 2021
López Ribalda and Others v. Spain [GC], nos. 1874/13 and 8567/13, 17 October 2019
Lüdi v. Switzerland, no. 12433/86, Series A no. 238
Lupker and Others v. the Netherlands, 18395/91, Commission decision, 7 December 1992

—M—

M.B. v. France, no. 22115/06, 17 December 2009
M.C. v. the United Kingdom, no. 51220/13, 30 March 2021
M.D. and Others v. Spain, no. 36584/17, 28 June 2022
M.G. v. the United Kingdom, no. 39393/98, 24 September 2002
M.K. v. France, no. 19522/09, 18 April 2013
M.L. and W.W. v. Germany, nos. 60798/10 and 65599/10, 28 June 2018
M.M. v. the United Kingdom, no. 24029/07, 13 November 2012
M.N. and Others v. San Marino, no. 28005/12, 7 July 2015
M.P. v. Portugal, no. 27516/14, 7 September 2021
M.S. v. Sweden, 27 août 1997, *Reports of Judgments and Decisions* 1997-IV
MGN Limited v. the United Kingdom, no. 39401/04, 18 January 2011
Magyar Helsinki Bizottság v. Hungary [GC], no. 18030/11, ECHR 2016
Malanicheva v. Russia (dec.), no. 50405/06, 31 May 2016
Malone v. the United Kingdom, 2 August 1984, Series A no. 82
Marchiani v. France (dec.), no. 30392/03, 27 May 2008

Matheron v. France, no. 57752/00, 29 March 2005
McGinley and Egan v. the United Kingdom, 9 June 1998, *Reports of Judgments and Decisions* 1998-III
McVeigh, O'Neill and Evans v. the United Kingdom, nos. 8022/77 and two others, Commission report, 18 March 1981
Mediengruppe Österreich GmbH v. Austria, no. 37718/18, 26 April 2022
Mehmedovic v. Switzerland (dec.), no. 17331/11, 11 December 2018
Mentzen v. Latvia (dec.), no. 71074/01, ECHR 2004-XII
Messina v. Italy (no. 2), no. 25498/94, ECHR 2000-X
Michaud v. France, no. 12323/11, ECHR 2012
Mik and Jovanović v. Serbia (dec.), nos. 9291/14 and 63798/14, 23 March 2021
Mikulić v. Croatia, no. 53176/99, ECHR 2002-I
Mifsud v. Malta, no. 62257/15, 29 January 2019
Mityanin and Leonov v. Russia, nos. 11436/06 and 22912/06, 7 May 2018
Mockutė v. Lithuania, no. 66490/09, 27 February 2018
Modestou v. Greece, no. 51693/13, 16 March 2017
Montera v. Italy (dec.), no. 64713/01, 9 July 2002
Moskalev v. Russia, no. 44045/05, 7 November 2017
Mosley v. the United Kingdom, no. 48009/08, 10 May 2011
Murray v. the United Kingdom [GC], 28 October 1994, Series A no. 300-A
Murtazaliyeva v. Russia [GC], no. 36658/05, 18 December 2018
Mustafa Sezgin Tanrıkulu v. Turkey, no. 27473/06, 18 July 2017

—N—

N. Š. v. Croatia, 10 September 2020
Nada v. Switzerland [GC], no. 10593/08, ECHR 2012
Nagla v. Latvia, no. 73469/10, 16 July 2013
National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France, nos. 48151/11 and 77769/13, 18 January 2018
News Verlags GmbH & Co.KG v. Austria, no. 31457/96, ECHR 2000-I
Niedbała v. Poland, no. 27915/95, 4 July 2000
Nuh Uzun and Others v. Turkey, nos. 49341/18 et seq., 29 March 2022

—O—

Odièvre v. France [GC], no. 42326/98, ECHR 2003-III
Oleynik v. Russia, no. 23559/07, 21 June 2016

—P—

P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001-IX
P.N. v. Germany, no. 74440/17, 11 June 2020
P.T. v. the Republic of Moldova, no. 1122/12, 26 May 2020
P. and B. v. the United Kingdom, no. 36337/97 and 35974/97, ECHR 2001-III
P. and S. v. Poland, no. 57375/08, 30 October 2012
Panteleyenko v. Ukraine, no. 11901/02, 29 June 2006
Peck v. the United Kingdom, no. 44647/98, ECHR 2003-I
Peers v. Greece, no. 28524/95, ECHR 2001-III
Pendov v. Bulgaria, no. 44229/11, 26 March 2020

Peruzzo and Martens v. Germany (dec.), nos. 7841/08 and 57900/12, 4 June 2013
Perry v. the United Kingdom, no. 63737/00, ECHR 2003-IX (extracts)
Petrova v. Latvia, no. 4605/05, 24 June 2014
Pinto Coelho v. Portugal (no. 2), no. 48718/11, 22 March 2016
Polanco Torres and Movilla Polanco v. Spain, 34147/06, 21 September 2010
Prado Bugallo v. Spain, no. 58496/00, 18 February 2003
Pruteanu v. Romania, no. 30181/05, 3 February 2015

—R—

R.E. v. the United Kingdom, no. 62498/11, 27 October 2015
Radio Twist, a.s. v. Slovakia, no. 62202/00, ECHR 2006-XV
Radu v. the Republic of Moldova, no. 50073/07, 15 April 2014
Rees v. the United Kingdom, no. 9532/81, Series A no. 106
Reklos and Davourlis v. Greece, no. 1234/05, 15 January 2009
Ricci v. Italy, no. 30210/06, 8 October 2013
Robathin v. Austria, no. 30457/06, 3 July 2012
Roche v. the United Kingdom [GC], no. 32555/96, ECHR 2005-X
Roemen and Schmit v. Luxembourg, no. 26419/10, ECHR 2003-IV
Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015
Rook v. Germany, no. 1586/15, 25 July 2019
Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V

—S—

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008
S.V. v. Italy, no. 55216/08, 11 October 2018
Sanoma Uitgevers B.V. v. the Netherlands [GC], no. 38224/03, 14 September 2010
Samoylova v. Russia, no. 49108/11, 14 December 2021
Šantare and Labazņikovs v. Latvia, no. 34148/07, 31 March 2016
Särgava v. Estonia, no. 698/19, 16 November 2021
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, ECHR 2017 (extracts)
Schmidt v. Germany (dec.), no. 32352/02, 5 January 2006
Sciacca v. Italy, no. 50774/99, ECHR 2005-I
Sedletska v. Ukraine, no. 42634/18, 1 April 2021
Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, ECHR 2006-VII
Sérvulo & Associados - Sociedade de Advogados, RL, and Others v. Portugal, no. 27013/10, 3 September 2015
Sheffield and Horsham v. the United Kingdom, 30 July 1998, *Reports of Judgments and Decisions* 1998-V
Sher and Others v. the United Kingdom, no. 5201/11, ECHR 2015 (extracts)
Shimovolos v. Russia, no. 30194/09, 21 June 2011
Silver and Others v. the United Kingdom, 25 March 1983, Series A no. 61
Sinan Işık v. Turkey, no. 21924/05, ECHR 2010
Smirnov v. Russia, no. 71362/01, 7 June 2007
Smith and Grady v. the United Kingdom, no. 33985/96 and 33986/96, *Reports of Judgments and Decisions* 1999-VI
Société de Conception de Presse and d'Édition v. France, no. 4683/11, 25 February 2016
Söderman v. Sweden [GC], no. 5786/08, ECHR 2013
Sommer v. Germany, no. 73607/13, 27 April 2017

Sõro v. Estonia, no. 22588/08, 3 September 2015
Standard Verlagsgesellschaft mbH v. Austria (no. 3), no. 39378/15, 7 December 2021
Stolkosa v. Poland (dec.), no. 68562/14, 14 September 2021
Succession Kresten Filtenborg Mortensen v. Denmark (dec.), no. 1338/03, ECHR 2006-V
Suprunenko v. Russia (déc), no. 8630/11, 19 June 2018
Surikov v. Ukraine, no. 42788/06, 26 January 2017
Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016
Szuluk v. the United Kingdom, no. 36936/05, ECHR 2009

—T—

Taylor-Sabori v. the United Kingdom, no. 47114/99, 22 October 2002
Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, no. 39315/06, 22 November 2012
Thoma v. Luxembourg, no. 38432/97, ECHR 2001-III
Tillack v. Belgium, 20477/05, 27 November 2007
Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), nos. 3002/03 and 23676/03, ECHR 2009
Toma v. Romania, no. 42716/02, 24 February 2009
Tønsbergs Blad A.S. and Haukom v. Norway, no. 510/04, 1er March 2007
Trabajo Rueda v. Spain, no. 32600/12, 30 May 2017
Trajkovski and Chipovski v. North Macedonia, nos. 53205/13 and 63320/13, 13 February 2020

—U—

Ungváry and Irodalom Kft. v. Hungary, no. 64520/10, 3 December 2013
Uzun v. Germany, no. 35623/05, ECHR 2010 (extracts)

—V—

Valašinas v. Lithuania, no. 44558/98, ECHR 2001-VIII
Valenzuela Contreras v. Spain, no. 2767/95, *Reports of Judgments and Decisions* 1998-V
Van der Velden v. the Netherlands (dec.), no. 29514/05, ECHR 2006-XV
Van Vondel v. the Netherlands, no. 38258/03, 25 October 2007
Vasil Vasilev v. Bulgaria, no. 7610/15, 16 November 2021
Vasylchuk v. Ukraine, no. 24402/07, 13 June 2013
Verlagsgruppe Droemer Knaur GmbH & Co. KG v. Germany, 35030/13, 19 October 2017
Vetter v. France, no. 59842/00, 31 May 2005
Vicent Del Campo v. Spain, no. 25527/13, 6 November 2018
Vinci Construction and GTM Génie Civil and Services v. France, nos. 63629/10 and 60567/10, 2 April 2015
Visy v. Slovakia, no. 70288/13, 16 October 2018
Volodina v Russia (no. 2), no. 40419/19, 14 September 2021
Von Hannover v. Germany, no. 59320/00, ECHR 2004-VI
Von Hannover v. Germany (no. 2) [GC], nos. 40660/08 and 60641/08, ECHR 2012
Vučina v. Croatia (dec.), no. 58955/13, 24 September 2019
Vukota-Bojić v. Switzerland, no. 61838/10, 18 October 2016

—W—

W. v. the Netherlands (dec.), no. 20689/08, 20 January 2009
Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI
Węgrzynowski and Smolczewski v. Poland, no. 33846/07, 16 July 2013
Wieser and Bicos Beteiligungen GmbH v. Austria, no. 74336/01, ECHR 2007-IV
Willems v. the Netherlands (dec.), no. 57294/16, 9 November 2021
Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no. 2) (dec.), no. 62746/00, ECHR 2002-X
Wisse v. France, no. 71611/01, 20 December 2005

—X—

X and Others v. Russia, nos. 78042/16 and 66158/14, 14 January 2020

—Y—

Y. v. Turkey (dec.), no. 648/10, 17 February 2015
Y.B. and Others v. Turkey, nos. 48173/99 and 48319/99, 28 October2004
Y.G. v. Russia, no. 8647/12, 30 August 2022
Y.Y. v. Russia, no. 40378/06, 23 February 2016
Yonchev v. Bulgaria, no. 12504/09, 7 December 2017
Youth Initiative for Human Rights v. Serbia, no. 48135/06, 25 June 2013
Yvonne Chave née Jullien v. France, no. 14461/88, Commission decision of 9 July 1991

—Z—

Z v. Finland, 25 February 1997, *Reports of Judgments and Decisions* 1997-I
Zoltán Varga v. Slovakia, nos. 58361/12 and 2 others, 20 July 2021