THE AIRE CENTRE
Advice on Individual Rights in Europe

CIVIL RIGHTS DEFENDERS

Balancing Data Protection with Transparent Justice

The European Legal Framework

THE AIRE CENTRE
Advice on Individual Rights in Europe

CIVIL RIGHTS DEFENDERS

Balancing Data Protection with Transparent Justice

The European Legal Framework

Editors

Biljana Braithwaite, Western Balkans Programme Director, the AIRE Centre
Catharina Harby, Senior Legal Consultant, the AIRE Centre
Goran Miletić, Director for Europe and MENA, Civil Rights Defenders

Main contributors

Ledi Bianku, former Judge at the European Court of Human Rights and Associate Professor, University of Strasbourg
Hannah Smith, Pupil Barrister, Doughty Street Chambers

We are very grateful to **Dechert LLP**, **Ishaani Shrivastava**, Barrister at Devereux Chambers, **Florence Powell**, Solicitor and Legal Project Manager at the AIRE Centre, and **Sihana Cara**, Trainee Solicitor at Herbert Smith Freehills, as well as **Robert Ford** for their contributions to the publication.

Print run
100

This original English version has also been translated into Bosnian/Croatian/Montenegrin/Serbian, Albanian and Macedonian

Design by
Kliker Dizajn

Printed by
Kuća Štampe Plus

Preface

Transparency of the courts is one of the strongest safeguards of an independent and impartial judicial system. The transparent administration of justice enables public commentary and criticism of judicial proceedings, increases public understanding of and trust in the judiciary, and builds wider confidence in the courts and the other democratic institutions that courts hold to account.

However, the ever-evolving technologies used in the context of investigative and judicial proceedings raise novel and complex questions regarding how most effectively to guarantee the fair, efficient and transparent administration of justice, whilst also capitalising on the potential benefits of new technologies.

Where innovative methods are used to investigate crime, the legitimate interest of protecting national security and fighting crime must be balanced with the protection of the right to private life of those who are the subject of targeted or bulk surveillance measures. When State authorities prosecute on the basis of evidence obtained through surveillance or intercepted communications, they are often unwilling to disclose the exact provenance of such material, or even to reveal its content at all, for fear of undermining the efficacy of a covert investigative tool. Such unwillingness has clear and potentially severe consequences for the right to a fair and public hearing and equality of arms.

The question of how best to balance these vital yet competing interests has been brought to the forefront as courts and State authorities grapple with questions concerning the admissibility of evidence obtained from the interception of EncroChat, Sky ECC, ANOM and other such devices. Such intercepted communications evidence has been used to investigate and prosecute 1,000s of people across Europe, including many in the Western Balkans. It is a practice that has been praised and berated in equal measure, celebrated by those who see it as a critical tool in the fight against crime, but criticised by those with concerns regarding the impact on the right to a fair hearing.

Regardless of one's view on the matter, what is clear is that it is acutely important for courts and lawyers in the Western Balkans to further their understanding of these novel means by which to collect evidence. The wealth of evidence and information collected from intercepted communications has the potential to galvanise efforts to prevent and punish serious and organised crime in the region. However, it is necessary

to develop a principled and pragmatic approach to balancing the many and varied interests at play, to ensure any eagerness to rely on this evidence to combat crime does not simultaneously undermine fairness of and trust in the judicial system.

In this context, as in many others, legal developments have struggled to keep pace with the technological developments they seek to regulate. At the time of writing, we await key judgments from the Strasbourg and Luxembourg courts which, it is hoped, will provide much needed further guidance on the topic. In the meantime, this publication elucidates the existing, relevant legal principles.

Technological developments are also impacting the ways in which courts conduct and communicate about judicial proceedings. This raises equally pressing questions regarding how best to safeguard the public nature of judicial proceedings and the public communication of judgments (both of which are fundamental aspects of the rights to a fair trial and to freedom of expression), whilst also protecting the right to private life, the presumption of innocence and the right to be forgotten of those involved. In addition, courts must publish and explain their decisions to build public trust and understanding in the judicial system. However, inaccurate, confusing or misleading coverage of a decision equally has the potential to undermine confidence in the courts.

Developing an understanding of the rights and obligations under Articles 6, 8 and 10 of the European Convention on Human Rights is, therefore, an essential first step to ensuring each of the many and varied interests in this sphere are protected. However, the work of the courts in securing transparent justice lies not only in understanding and applying the relevant caselaw, but also in building constructive relationships with the media, developing careful and coherent communication strategies and implementing policies regulating the publication and anonymisation of judgments.

We hope that this publication will serve to further both the legal and the practical knowledge required to take such a holistic approach. We also hope this publication will inspire judges and lawyers in the region to continue to undertake the difficult, but necessary, task of integrating new technologies and practices into their work, to profit from all the benefits they can offer, without compromising on the fundamental guarantees provided for under Articles 6, 8 and 10.

Biljana Braithwaite
Western Balkans Programme
Director, the AIRE Centre

Goran Miletić
Director for Europe and MENA,
Civil Rights Defenders

Contents

PART 2 - Case Summaries: 115

LIST OF ACRONYMS

The following table describes the significance of various abbreviations and acronyms used throughout the handbook.

Abbreviation	Definition
ECHR / the Convention	The European Convention on Human Rights
The Court / the ECtHR	The European Court of Human Rights
CJEU	The Court of Justice of the European Union
EEA	European Economic Area
EDPS	The European Data Protection Supervisor
State(s)/ Contracting State(s)	Contracting State(s) of the European Convention on Human Rights
ICJ	International Court of Justice
ICCPR	International Covenant on Civil and Political Rights
Convention 108	The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
Convention 108+	Amending Protocol to the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Protocol CETS No. 223)
GDPR	General Data Protection Regulation
TFEU	Treaty on the Functioning of the European Union
Budapest Convention	The Convention on Cybercrime (ETS No. 185)
DPC	The Data Protection Commissioner of the Council of Europe
IP	Internet Protocol
ISP	Internet Service Provider
SIAC	Special Immigration Appeals Commission

PART 1

Introduction

This publication is divided into two Parts. Part 1 consists of the narrative and Part 2 consists of summaries of selected judgments and decisions of the European Court of Human Rights (the "Court" or the "ECtHR").

Data protection and privacy, in respect of individuals' private information, is a growing area. The legal instruments and case law are ever evolving as they seek to maintain pace with the fast-paced developments in modern technology, as more personal data is produced, recorded, and used. Technology opens countless possibilities – most notably to enhance and develop individuals' and organisations' interactions with each other. However, as the technology develops, and the public's and State's interaction with technology increases, new human rights issues will continue to arise, which both domestic and international courts and legal instruments will have to address.

Part 1 of this publication looks to analyse these potential human rights issues in respect of data protection and privacy of information in the context of judicial proceedings. It looks at the investigations that may precede proceedings, issues that may arise during proceedings, and afterwards in the pronouncement of judgments, and also considers the growing case law on the 'right to be forgotten' for those involved in judicial investigations and proceedings.

The publication considers both prior case law and looks forward to potential issues that may arise as technology continues to develop and be used. For instance, in considers the use of by State authorities of technology to intercept encrypted communications and the human rights challenges that this may give rise to, including where data is shared between States.

The focus is on the European Convention of Human Rights (the "ECHR" or the "Convention") and the case law of the ECtHR, as well as other legal instruments of the Council of Europe. However, the publication also considers developments

in European Union ("EU") law and the judgments of the Court of Justice of the European Union (the "CJEU"). EU law and CJEU jurisprudence is relevant for the Western Balkans not only due to the issue of accession, but also because the ECtHR takes account of CJEU jurisprudence and EU instruments – and this has been particularly notable in the context of data protection.

The narrative in Part 1 is divided into six subsections. Following this Introduction, the **second subsection** is an overview of the relevant legal instruments in this area. These are subdivided into Council of Europe instruments and European Union instruments. This subsection also considers the roles of the Council of Europe Data Protection Commissioner and the European Data Protection Supervisor.

In respect of the ECHR, this subsection explains how the protection of personal data is not a separate right under the ECHR, however the control of information about oneself, and thus data protection, has been found by the ECtHR to be of fundamental importance to the right to respect for private and family life guaranteed by Article 8 ECHR. The ECtHR's jurisprudence in this area is voluminous across a wide range of contexts, from secret surveillance conducted by public authorities to combat organised crime to use of personal data as evidence in the judicial context. Safeguards against abuse and arbitrariness are key, specifically those delineating the limits within which authorities may operate and providing for compensation and redress.

The right to a fair trial under Article 6 ECHR, may also have a role where a person's personal data has been processed in the context of judicial proceedings. However, Article 6 can conflict with Article 8 in the context of data protection and judicial proceeding – for instance in respect of the right to a public hearing and the right to the public pronouncement of judgments. Further, the right to freedom of expression under Article 10 ECHR is often engaged. This right may stand in conflict to Article 8 in the context of data protection – for instance in respect of the right to be forgotten – and national authorities and courts must strike a fair balance between the two rights. Analysis of these rights and potential conflicts is provided in later subsections of the Guide.

This subsection also considers, amongst other instruments, the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – a landmark instrument which aims to empower individuals to know about, understand and control the processing of their personal data by others whilst providing a framework for international data flows,

and subsequent modernising protocols, which address challenges resulting from the use of new information and communication technologies.

In respect of European Union instruments, the most notable is the Charter of Fundamental Rights of the European Union, under which Article 7 concerns the respect for private and family life, and Article 8 contains a specific protection of person data. Also of particular relevance is the EU General Data Protection Regulation (GDPR), which modernised EU data protection legislation and provided for consistent rules across the Member States.

The **third subsection** examines in more detail the question of what constitutes private information and personal data. It considers how, and when, the collection, storage, alteration, disclosure, use and publication of information relating to an individual's private life can represent an interference with Article 8 ECHR. The ECtHR has developed extensive jurisprudence on what can amount to personal data. Examples of such information and data are given from the case law of the ECtHR, including case law on data which is in the public domain and more 'sensitive' personal data.

The **fourth subsection** covers the protection of private information during the investigative phase of proceedings. State authorities might seek to collect personal data in a variety of different contexts related to the judiciary, for example as part of attempts to combat crime, and to collect evidence for use in prosecutorial and judicial proceedings. This subsection considers examples of such measures that States may adopt, including the search and seizure of personal data, secret surveillance, bulk interception and targeted interception of communications, and the infiltration of encrypted communications, and how these measures might constitute an interference with Article 8 ECHR.

As technology develops the extent of data that may be collected by States will only increase, with the corresponding increase in potential interferences with Article 8 ECHR. In respect of bulk interception of communication, which do not target any specific individual, for instance, these measures have a potentially extraordinarily wide reach both inside and outside the State conducting the surveillance. Likewise, the use of software by State authorities to infiltrate encrypted communications has raised several potential human rights issues, including in respect of States intercepting the messages of senders based in other countries and the transfer of data across jurisdictions.

There is a particularly increased risk of abuse in respect of secret surveillance. Due to their very nature, the existence and application of secret surveillance measures can remain unknown to those impacted by them and State authorities will be unwilling to disclose details of, or the existence of, surveillance as this would undermine its effectiveness. This subsection therefore analyses how the ECtHR has sought to recognise the necessarily secret nature of these surveillance measures, whilst also limiting the potential for abuse and ensuring that measures can be challenged. This subsection emphasises the importance of the existence, and effective implementation, of adequate guarantees against the abuse of data collection powers.

The fourth subsection also provides analysis of when the use of material obtained in breach of Article 8 in judicial proceedings may engage questions of the right to a fair trial under Article 6. This subsection notes how the use of such evidence in judicial proceedings will not automatically give rise to a breach of Article 6 and the ECtHR has reiterated that the rules on admissibility of evidence is primarily a matter for domestic law. The question is whether the proceedings as a whole are fair, considering all the circumstances of the case, including whether the applicant is able to challenge the admissibility of the evidence in an adversarial process.

There are numerous other ways in which the guarantees provided by Article 6 might be impacted by the requirements to protect personal data under Article 8. The **fifth subsection** therefore addresses the publication of information during judicial proceedings and the interactions between Article 8 and Article 6 in this context. This section is subdivided into consideration of the presumption of innocence under Article 6, protections under Article 8, the right to a public hearing under Article 6, and the right to public pronouncement of judgments under Article 6.

First, this subsection considers the investigative stage of judicial proceedings and how Convention rights, might be engaged when information is shared with the public about those proceedings. In this context the right to be presumed innocent until proven guilty under Article 6(2) is of particular importance in relation to criminal proceedings, for instance where, public statements could include premature assertions that the accused is guilty.

The public nature of judicial proceedings can give rise to concerns regarding the protection of the confidentiality of a person's personal data, which might be discussed or disclosed at a public hearing. Analysis is included of the ECtHR's case

law on how national authorities must strike a fair balance between the public character of proceedings, which the ECHR recognises as a fundamental principle of democratic society, and protecting the interests of a party (or third party) to proceedings in maintaining confidentiality of their data, for instance by limiting the type and scope of data disclosed at a hearing, or, in certain circumstances, holding a hearing in camera.

Analysis is also provided on the circumstances when the public pronouncement of judgments, which is a freestanding right under Article 6, may be limited, for instance in national security cases. The public pronouncement of a judgment also has the potential to infringe upon the rights to the protection of personal data, physical and moral integrity, reputation and honour of those who are referenced in a judgment; and a balance must be struck between a fair trial and data protection. The different approaches to requests for anonymity before the ECtHR and the CJEU are also considered, along with a comparison to the approaches taken in the UK and German courts.

This leads Part 1 of the publication to its **final section** which focuses on the evolving concept of the 'right to be forgotten' and the right to erasure of data. This section considers the various sources of the 'right to be forgotten', which, in the ECHR context, is not a free-standing right but can form part of Article 8. In the context of investigative and judicial proceedings, cases on the 'right to be forgotten' have arisen in two broad contexts. First, cases stemming from the operation of the State's criminal and civil justice system and associated record-keeping, for instance the keeping of records of individuals suspected of committing an offence, but who are never convicted. Secondly, cases concerning journalistic content published about individuals who have been the subject of criminal or civil investigations or proceedings.

This latter category can raise particular issues in respect of freedom of expression and freedom of the press, especially as, with the development of technology and communication tools, a person's personal information that is published online has the potential to be available for some time and can have far-reaching consequences. This final subsection therefore addresses in depth the competing considerations between the right to privacy and freedom of expression as they arise in the context of the 'right to be forgotten'.

Part 2 of this publication, includes summaries of the judgments of the Court that are considered relevant to the topic dealt with. In this instance, that includes cases at ECtHR cases as well as judgments of the CJEU.

Chapter 1

Overview of relevant legal instruments

There are various instruments and authorities at the European level concerning data protection and the data protection obligations which apply in the context of investigative and judicial proceedings. This section outlines some of the major legal instruments, including the relevant Articles within each.

a) Council of Europe instruments

European Convention of Human Rights

The protection of personal data is not a separate right under the European Convention of Human Rights ("**ECHR**", or "**the Convention**").[1] However, the European Court of Human Rights ("**ECtHR**") has found that data protection is of vital importance to a person's enjoyment of their rights guaranteed by Article 8 ECHR.[2] This is the main Article through which the ECHR protects personal data.

Article 8

Article 8, which protects the right to respect for private and family life, states:

> *"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*

[1] See below and compare with Article 8 of the Charter of Fundamental Rights of the EU.

[2] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, Grand Chamber judgment of 27 June 2017, no. 931/13, §137; *Z v. Finland*, judgment of 25 February 1997, no. 22009/93 at §95.

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."

The primary purpose of Article 8 is to protect against arbitrary interferences by public authorities with private and family life, home and correspondence. To demonstrate a breach of Article 8, an applicant must show that their complaint falls within at least one of the four interests protected by the Article, namely, private life, family life, home, and correspondence. In relation to all four interests, the ECtHR has defined the scope of Article 8 broadly, including in the context of data protection.[3] The ECtHR's jurisprudence on the collection and use of personal data is voluminous and covers a wide range of situations, from secret surveillance conducted by public authorities to combat organised crime to the use of personal data as evidence in the judicial context.

The Court has clearly indicated 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, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article… Article 8 of the Convention thus 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 their Article 8 rights may be engaged."[4]

The State may only interfere with a right protected by Article 8 where it is (a) in accordance with the law, (b) in pursuit of a legitimate aim, and (c) necessary in a democratic society in respect of one of the interests listed in Article 8(2). Additionally, the State is obliged to ensure Article 8 rights are respected in the context of relations between private parties e.g. by adopting specific measures aimed at doing so.

---

[3] See for example *Klass and Others v. Germany*, judgment of 6 September 1978, no. 5029/71 at §41 (included as a summary in this publication).

[4] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, Grand Chamber judgment of 27 June 2017, no. 931/13 at §137.

The requirements of Article 8 in respect of data protection are considered in detail below. However, by way of example, in *Zoltan Varga v. Slovakia*,[5] the ECtHR considered the compatibility of secret surveillance with Article 8. In this case, the applicant was the subject of surveillance aimed at monitoring him and the meetings taking place at a property he owned. The warrants authorising the surveillance were subsequently annulled, and some surveillance material was anonymously posted online.

The ECtHR found that the covert surveillance amounted to a violation of the applicant's right to private life on the sole basis that the interference with his Article 8 rights was not "in accordance with law", without finding it necessary to examine whether the interference served a legitimate aim. The following factors were relevant to this finding:

- the warrants were subsequently annulled by the domestic courts on the basis that they were unlawful and unconstitutional;
- there was no examination by the issuing court of whether the grounds for surveillance continued to exist as required by statute;
- the court files regarding the warrants had been destroyed;
- there were no specific rules governing the implementation of the warrants or the destruction of the material obtained;
- control of the Slovak Intelligence Service (SIS) was mainly political; no commission to supervise had been set up and the domestic courts had not reviewed the actions of the SIS;
- the implementation of the warrants was outside the purview of the administrative-law judiciary and beyond the scope of state liability legislation; and
- the retention of the surveillance material had no sufficient basis in law, and the storing of surveillance material had been subject to confidential rules adopted and applied by the SIS with no element of external control.

As demonstrated by this judgment, safeguards against abuse and arbitrariness in the collection and processing of personal data are key, specifically those delineating the limits within which authorities may operate and providing opportunities for review and redress where it is believed those limits have been crossed.

[5] *Zoltan Varga v. Slovakia*, judgment of 20 July 2021, nos. 58361/12, 25592/16 and 27176/16.

Of particular relevance for judges and prosecutors, are the issues of data protection that come into play during judicial proceedings.[6] In addition to their rights under Article 8 ECHR, any person whose personal data is collected and processed in the context of judicial proceedings must also enjoy the guarantees of Article 6.

Article 6

Article 6, concerning the right to a fair trial, states:

> *"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*

[6] See, as recent examples, *Ships Waste Oil Collector B.V. v. the Netherlands*, judgment of 16 May 2023, no. 2799/16 (included as a summary in this publication), and *Janssen de Jong Groep B.V. and Others v. the Netherlands*, judgment of 16 May 2023, no. 2800/16, not yet final at the moment of writing this Guide.

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."

Eternit v. France[7] is an example of the balance to be struck between Article 6 and Article 8 in the data protection sphere. Here, the applicant company complained that Article 6 had been violated when it was not provided with the medical information relied upon by a consulting doctor for the Health Insurance Office to conclude that an employee of the applicant company had contracted an occupation-related disease.

The ECtHR found that the claim was inadmissible (manifestly ill-founded). The civil limb of Article 6 was found to be engaged where an employer challenged a decision of a Health Insurance Office that a disease was occupation-related. However, the right to an adversarial procedure under Article 6 must be balanced against the right to medical confidentiality in such a way that neither is impaired in its very essence. The Court suggested one way to respect both Articles 6 and 8 could be for the domestic court to appoint an independent medical expert to review the relevant medical records to guide the court and the parties without breaching the confidentiality of those medical records. This mechanism is not, however, required every time an employer requests it; it is sufficient for an independent expert to be appointed only when the court considers that it has insufficient information. The ECtHR also noted that the doctor in this case was not under the direct authority of the Health Insurance Office, and that the procedure by which the latter reached its decision was generally in line with the adversarial principle.

In addition to Articles 8 and 6 ECHR, in several cases data protection issues have been examined also under Article 10 ECHR.

[7] *Eternit v. France*, judgment of 27 March 2012, no. 20041/10.

Article 10

Article 10, on the right to freedom of expression, provides:

> *"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."*

The ECtHR has held that "freedom of expression constitutes one of the essential foundations of [democratic] society, one of the basic conditions for its progress and for the development of every man".[8]

Article 10 is broad in scope. Its protections are not limited to particular types of information or ideas, or forms of expression. It applies equally to, for example, paintings, the production of plays, information of a commercial nature, photos and photomontages, and conduct.

The ECtHR has stressed that Article 10 protects information and ideas that offend, shock or disturb, not merely those that are inoffensive or a matter of indifference; but incitement to intolerance or violence and hatred are legitimate limits on Article 10.

In the context of data protection, Article 8 and Article 10 might be viewed as standing in opposition to one another. In balancing the rights protected under each Article, the ECtHR has found that the outcome of a case should in principle not depend on the Article under which the complaint was lodged.

---

[8] *Handyside v. the United Kingdom*, judgment of 7 December 1976, no. 5493/72 at §49.

The judgment of *Dupuis and others v. France*[9] is an illustration of balancing Article 6 and Article 10 rights in relation to the publication of material obtained from an ongoing judicial investigation. In this case, the applicants – two journalists and a publishing company – were found guilty of the offence of using information obtained illegally (through a breach of the confidentiality of the investigation or of professional confidentiality) in their book describing the workings of surveillance operations ordered at the highest level of the state. The surveillance operations had provoked considerable media interest when they were discovered. During a judicial investigation, one of the French President's main aides, GM, was placed under formal investigation; it was he who lodged the complaint leading to the applicants' conviction.

The ECtHR accepted that the conviction was prescribed by law and had a legitimate aim. In respect of the necessity of the interference, on the one hand, the applicants' book contributed to a debate of considerable public interest and the public had a legitimate interest in the information it contained e.g. against whom surveillance had been ordered, the conditions of surveillance and the instigators. GM was not a politician, but was an influential public figure. On the other hand, it is legitimate to grant special protection to the confidentiality of the judicial investigation. However, at the time of the publication of the book, there was already widespread media coverage and it was well-known that GM was under investigation; indeed, he regularly made comments to the press. It had not, therefore, been established how disclosure in the book could have had a negative impact on GM's right of presumption of innocence. The journalists had acted in accordance with the standards governing their profession. The ECtHR found that there was a violation of Article 10.

In *N.S. v. Croatia*,[10] the applicant was found guilty of breaching the confidentiality of administrative proceedings relating to the custody of a child by disclosing confidential information. Following a tragic accident, there was a dispute between the paternal and maternal family about the custody of NG, a child. This attracted significant media coverage. The applicant had given interviews, including on national television, in which she had provided information obtained from the confidential custody proceedings; as a result, she was found guilty.

[9] *Dupuis and others v. France*, judgment of 7 June 2007, no. 1914/02.

[10] *N.S. v. Croatia*, judgment of 10 September 2010, no. 36908/13.

The ECtHR considered whether the interference with Article 10 was necessary in a democratic society. The applicant's right to inform the public about the improper functioning of child care proceedings – she had acted in good faith to protect NG's interests – had to be balanced against NG's right to privacy and against the prohibition on disclosure without authorisation of information revealed during proceedings held in private. The ECtHR found that the national courts had applied a formalistic approach to confidentiality. The protection of children's personal data was essential; however, no consideration had been given to the background of the disclosure and the fact that the information disclosed was already in the public domain, at times provided by the domestic authorities themselves.

Convention 108 and Convention 108+

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) ("**Convention 108**") is a landmark instrument in the field of data protection adopted by the Council of Europe in January 1981.[11] Convention 108 aims to empower individuals to know about, understand and control the processing of their personal data by others whilst providing a framework for international data flows. It does so by laying down conditions and restrictions in respect of the processing of information and the protection of personal data, and fostering international co-operation between supervisory authorities. It strikes a delicate balance between the right to personal autonomy and human dignity, on one hand, and, on the other, the importance of global data flows in exercising fundamental rights and fostering social and economic progress.[12]

The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181) (the "**Additional Protocol**") was adopted by the Council of Europe in November 2001. The aim of the Additional Protocol was to improve the application of the principles contained in Convention 108 in two main regards. Firstly, it provides for parties to set up national supervisory authorities responsible for ensuring compliance with the laws

[11] Convention 108 has been ratified by 55 states, including non-members of the Council of Europe, such as Uruguay, Tunisia and Mexico. In respect of the Western Balkan states, Albania ratified Convention 108 in 2005, Bosnia and Herzegovina in 2006, Montenegro in 2005, North Macedonia in 2006, and Serbia in 2005. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

[12] COE Convention 108+, p.16. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

adopted pursuant to Convention 108. Secondly, it restricts transborder data flows to third countries and/or international organisations that are able to afford an adequate level of protection.

In May 2018, the Committee of Ministers adopted the Amending Protocol to the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Protocol CETS No. 223) ("**Convention 108+**").[13] This aims to modernise Convention 108 (and the protocols adopted since 1981) to deal with challenges resulting from the use of new information and communication technologies and to strengthen its effective implementation.[14]

There are various differences between Convention 108 and Convention 108+. For example, the wording and structure of Article 1, detailing the objective and purpose, has been amended to "highligh[t] the fact that the processing of personal data may positively enable the exercise of other fundamental rights and freedoms".[15]

Whilst the definitions of personal data and data subjects were not modified by Convention 108+, further definitions were introduced, such as recipient and processor. Convention 108+ applies to both automated and non-automated processing of personal data; however, it continues to apply to both the private and public sectors indistinctly.[16]

Parties are no longer able to exempt certain types of data processing from the application of Convention 108+ e.g. for national security and defence purposes. The special categories of data (i.e. those which benefit from heightened protections) have been expanded to include genetic and biometric data, trade-union membership and ethnic origin. Data subjects are granted new rights to enable them greater control over their data, including the provision of further information when data subjects exercise their right of access and an entitlement to obtain knowledge of the reasoning underlying the data processing.[17]

---

[13] As at the date of writing, Convention 108+ has been ratified by 26 states so far and will come into force once it has been ratified by at least 38 states. Of the Western Balkan states, Serbia (2020), North Macedonia (2021) and Albania (2022) have ratified Convention 108+. Bosnia and Herzegovina is a signatory; however, Montenegro is not yet a signatory. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[14] COE Convention 108+, p.16, 34. https://www.coe.int/en/web/data-protection/convention108-and-protocol.

[15] Council of Europe, the modernised Convention 108: novelties in a nutshell: https://rm.coe.int/16808accf8, p.1.

[16] Council of Europe, the modernised Convention 108: novelties in a nutshell: https://rm.coe.int/16808accf8, p.2

[17] Council of Europe, the modernised Convention 108: novelties in a nutshell: https://rm.coe.int/16808accf8, p.3

The ECtHR has referred to Convention 108 in its case law concerning data protection, in particular, the Court relies on the definitions of personal data, data processing and sensitive / special categories which are set out in Convention 108.[18]

It is also to be noted that work on Convention 108+ and the EU data protection reform package "ran in parallel and utmost care was taken to ensure consistency between both legal frameworks."[19]

Recommendation No. R (95) 4

Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the protection of personal data in the area of telecommunication services, with particular reference to telephone services ("**Recommendation No. R (95) 4**") was adopted by the Committee of Ministers on 7 February 1995.

This instrument seeks to apply the principles of Convention 108 to the sector of telecommunications, in particular telephony, to guarantee an individual's privacy when using telecommunication services. It offers specific rules and guidelines for the sector to address the contemporary data protection vulnerabilities of telephone communications, such as unauthorised interception and greater personal data generation and storage. This was undertaken because it was felt that it was not immediately obvious how to find solutions compatible with Convention 108 to the problems raised by the new technology.

Budapest Convention

The Convention on Cybercrime (ETS No. 185) (the "**Budapest Convention**") is the first, and considered to be the most relevant, international treaty on cybercrime and electronic evidence. It opened for signature on 23 November 2001 and, as at the date of writing, has been ratified 68 countries in Europe, Africa, North and South America and Asia, including the United States of America.

The aim of the Budapest Convention is to support the development of a common criminal policy aimed at the protection of society against cybercrime,

[18] *Aman v. Switzerland*, Grand Chamber judgment of 16 February 2000, no. 27798/95; *Benedik v. Slovenia*, judgment of 24 April 2018, no. 62357/14; *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §§58-60

[19] Convention 108+ Explanatory Report, p.15. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

for example by encouraging the adoption of appropriate legislation and fostering international co-operation. As such, it provides for (i) the criminalisation of conduct ranging from illegal access, data and system interference to copyright infringement, computer-related fraud and child pornography; (ii) legal procedural tools to investigate cybercrime and secure electronic evidence; and (iii) efficient international cooperation.

The Budapest Convention strikes a balance between permitting societies to access and use the Internet freely and ensuring an effective criminal justice response to cybercrime. Any restrictions on computer and Internet use are defined narrowly; investigations and prosecutions are limited to specific criminal offences; and only specified data required as evidence in specific criminal proceedings is secured, subject to various safeguards.[20]

b) European Union instruments

The Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (the "**Charter**") contains 50 fundamental rights and principles, with four additional articles concerning the interpretation and application of the Charter. It has been legally binding since 1 December 2009 with the same legal value as other treaties of the European Union[21]. Whilst the Charter is always binding on the institutions, bodies, offices and agencies of the EU, Member States are only subject to it when implementing EU law[22].

Individuals, private legal persons and even public entities in certain circumstances may rely on the Charter in respect of their relations with EU institutions and bodies etc., and with Member States implementing EU law. [23]

[20] The ECtHR has referred in several judgments to the Convention on Cybercrime. See for example *K.U. v. Finland*, judgment of 2 December 2008,, no. 2872/02 at §§24-27.

[21] Article 6(1), the Treaty on European Union ("**TEU**").

[22] Article 51, the Charter.

[23] FRA, "Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level: guidance", 2020, p.20.

Article 7, concerning respect for private and family life, states:

> *"Everyone has the right to respect for his or her private and family life, home and communications."*

The Explanations relating to the Charter[24] provide that Article 7 corresponds to Article 8 ECHR. In light of technological developments, "communications" has been used in place of "correspondence" which is found in Article 8 ECHR. Under Article 52(3) (see below), the limitations which may legitimately be imposed on this right are the same as those permitted by Article 8 (2) ECHR.

In a similar manner to Article 8 ECHR, for Article 7 Charter to be engaged, there must be an interference with the right, which depends on the context and facts of each case.[25]

Article 8 of the Charter, which provides specifically for the protection of personal data, states:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority."*

There is no similar standalone right for the protection of personal data recognised by the ECHR. As discussed above, the right to protection of personal data is encapsulated within the right to private life under Article 8 ECHR. However, the drafters of the Charter felt that technological developments, together with the advancement of the international and national law, including case-law dealing specifically with data processing, called for a separate provision protecting this

[24] OJ C 303, 14.12.2007, pp. 17-35.

[25] FRA, "Handbook on European data protection law", 2018, p. 20.

right. The Court of Justice of the European Union ("**CJEU**") has explained that Articles 7 and 8 of the Charter are so closely linked that they may be regarded as establishing a 'right to respect for private life with regard to the processing of personal data'[26], with Article 8 taking the role of a lex specialis in relation to Article 7.[27]

Article 8 Charter is engaged as soon as personal data is processed. Unlike Article 7 Charter and Article 8 ECHR, there is no need to show that persons concerned have been inconvenienced in any way.

To be lawful, all data processing must fulfil the conditions laid down by Article 52(1) (see below). Article 52(1) imposes conditions of lawfulness and proportionality where any rights provided for in the Charter are limited, akin to those found in Article 8(2) ECHR. However, under the Charter, there is greater potential for such conditions to be applied to data processing, given that (by comparison to Article 8 ECHR) it is not necessary to show an interference with a person's rights; mere processing of personal data suffices to engage Article 8 Charter.

Article 52, regarding the scope and interpretation of rights and principles, states:

> *"1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*

---

[26] See *Volker und Markus Schecke GbR and others v. Land Hessen*, Grand Chamber judgment of 9 November 2010, Joined Cases C-92/09 and C-93/09 at §52.

[27] In this regard the CJEU has underlined that: "*The retention of data for the purpose of possible access to them by the competent national authorities… directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article…" Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others*, Grand Chamber judgment of 8 April 2014,– Joined Cases C-293/12 and C-594/12 at §29 (included as a summary in this publication).

…

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

…"

Under Article 52(3), while the ECHR establishes the minimum threshold of protection, EU law (including the Charter) may provide for more extensive protection. In respect of the Charter rights which correspond to the rights protected by the ECHR, those Charter rights have the same meaning and scope as those laid down by the ECHR, including by reference to the ECHR case law.[28]

In their case law, the CJEU and the ECtHR often refer to the other's judgments as part of the constant dialogue between the two courts. Therefore, CJEU jurisprudence is relevant for the Western Balkans not only due to the issue of accession, but also because the ECtHR takes account of CJEU jurisprudence and EU instruments, particularly in the context of data protection.

Digital Rights Ireland[29] is an example of how the CJEU has applied the Charter provisions on data protection in the field of the investigation and prevention of crime. This case is discussed below under Directive 2006/24/EC.

Directive 2006/24/EC

Directive 2006/24/EC concerned the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks. It required providers of publicly available electronic communication services or public communication networks to retain users' data for up to two years to permit the prevention, investigation

[28] FRA, "Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level: guidance", 2020, p.22.

[29] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others*, Grand Chamber judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 (included as a summary in this publication).

and prosecution of serious crime. The content of the electronic communications was not required to be stored.

In April 2014, the CJEU declared the directive to be invalid in *Digital Rights Ireland*[30] because it involved serious interferences with Article 7 and 8 Charter rights which were not strictly limited to what was necessary.

Digital Rights Ireland is therefore an example of how the CJEU has applied the Charter provisions on data protection in the field of the investigation and prevention of crime. In particular, the CJEU held that there had been an interference with Article 8 Charter because the directive required the processing of personal data. There had also been interference with Article 7 Charter because the data retained allowed for "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[31]

General Data Protection Regulation

The General Data Protection Regulation[32] ("**GDPR**") was adopted under Article 16 Treaty on the Functioning of the European Union ("**TFEU**"), and provides an independent legal basis for data protection which extends to all matters on which the EU is competent to legislate, including police and judicial cooperation in criminal matters. The GDPR modernised EU data protection legislation and provided for consistent rules across the Member States.[33]

---

[30] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others*, Grand Chamber judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 (included as a summary in this publication).

[31] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others*, Grand Chamber judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 at §27 (included as a summary in this publication).

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The Regulation entered into force on 25 May 2018.

[33] The GDPR repealed Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive). See also FRA, "Handbook on European data protection law", 2018, p.30.

Article 10

Article 10 GDPR, which concerns the processing of personal data relating to criminal convictions and offences, states:

> *"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) [the circumstances in which processing is lawful] shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."*

Applicability of the GDPR to courts

Recital 20 of the GDPR states:

> *"While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations." (emphasis added)*

This Recital sets out that whilst the GDPR applies to courts, the national supervisory authority required by the GDPR should not oversea the personal data processing undertaken by courts acting in their judicial capacity. This is detailed in the Articles of the GDPR which carve out exceptions to the general rules for courts acting in their judicial capacity.

Article 9 GDPR, on the processing of special categories of personal data, provides:

> *"1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*
>
> *2. Paragraph 1 shall not apply if one of the following applies:*
>
> *…*
>
> *(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;"*

Article 23 GDPR enumerates the situations in which states are permitted to restrict or make exemptions to the data protection obligations otherwise imposed under the GDPR. This includes where it is necessary and proportionate for:

> *…*
>
> *(f) the protection of judicial independence and judicial proceedings;"*

Article 37 GDPR, on the requirement of a data protection officer, states:

> *"1. The controller and the processor shall designate a data protection officer in any case where:*
>
> *a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;"*

Article 55 GDPR, on the competence of the supervisory authority required under Article 51, states:

> *"…*
>
> *3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity."*

It appears that 18 of the 30 European Economic Area ("**EEA**") Member States interpreted the phrase "acting in their judicial capacity" as meaning that courts can act in their judicial capacities, but can also act in other capacities. This is known as the functional interpretation. In contrast, only eight countries adhered to an interpretation that courts always act in their judicial capacities, known as the institutional interpretation.[34]

In regards to the functional interpretation, the practices of the EEA countries are homogenous. Personal data in all legal court cases are seen as within the scope of the judicial capacity. This means personal data in documents processed in such cases, including verdicts, case records etc. However, personal data not related to the contents of court cases, such as data relating to internal organisation and processes and personnel of the courts, are beyond the scope of judicial capacity. In the relevant countries, courts have arranged supervision internally when they are acting in their judicial capacity e.g. via courts higher in the hierarchy or special departments.[35]

In *X and Z v. Autoriteit Persoonsgegevens*[36], the CJEU appears to have adopted a functional interpretation. Z, a party to court proceedings represented by X, requested that the Dutch supervision authority take enforcement measures against the relevant judicial authority for infringement of the GDPR. They claimed the GDPR had been infringed when the judicial authority had made available to journalists present on the day of the hearing documents intended to enable journalists to follow hearings, namely a copy of the notice of appeal, a copy of the response and a copy of the contested judicial decision. Those documents were destroyed at the end of the day. The Dutch supervision authority refused as it was not competent under Article 55(3) GDPR i.e. because the judicial authority was acting in its judicial capacity.

The CJEU held that Article 55(3):

> *"must be understood… as not being limited to the processing of personal data carried out by courts in specific cases, but as referring,*

[34] Custers et al, "Quis custodiet ipsos custodies? Data protection in the judiciary in EU and EEA Member States" *International Data Privacy Law* (2022), pp.103, 108-111.

[35] Custers et al, "Quis custodiet ipsos custodies? Data protection in the judiciary in EU and EEA Member States" *International Data Privacy Law* (2022), p.111.

[36] *X and Z v. Autoriteit Persoonsgegevens*, First Chamber judgment of 24 March 2022, C-245/20.

more broadly, to all processing operations carried out by courts in the course of their judicial activity, such that those processing operations whose supervision by the supervisory authority would be likely, whether directly or indirectly, to have an influence on the independence of their members or to weigh on their decisions are excluded from that authority's competence."[37]

Thus, the processing of personal data carried out by courts in the context of their communication policy on cases before them falls outside the competence of the supervision authority. The determination of information from a case file to be shared with journalists to enable them to report on court proceedings is "clearly" linked to courts acting in their judicial capacity. It is irrelevant whether or not there is a legal basis in domestic law for courts to disclose information to third parties.[38]

c) Council of Europe Data Protection Commissioner

The Data Protection Commissioner of the Council of Europe ("**DPC**") is an independent function established under Article 4 of the Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe ("**1989 Regulation**").

The DPC ensures that all personal data collected and processed by the Council of Europe is in conformity with the data protection principles set out in the 1989 Regulation. The DPC also has other functions, including:

- investigating complaints from staff arising out of the implementation of the 1989 Regulation;
- formulating opinions at the request of the Secretary General on any matter relating to the implementation of the 1989 Regulation; and
- bringing to the attention of the Secretary General any proposals for improvement of the system of data protection.[39]

[37] *X and Z v. Autoriteit Persoonsgegevens*, First Chamber judgment of 24 March 2022, C-245/20 at §34.

[38] *X and Z v. Autoriteit Persoonsgegevens*, First Chamber judgment of 24 March 2022, C-245/20 at §§36-38.

[39] Council of Europe, Activity Report of the Data Protection Commissioner: November 2020-October 2022, DPCOM Report 2020-2022, p.5.

The DPC may also be invited to participate in the work of the Consultative Committee of Convention 108 and in meetings of bodies external to the Council of Europe, such as the Global Privacy Assembly.[40]

Between 2020 and 2022, the DPC participated, during the Global Privacy Assembly in Mexico, in a panel on Convention 108 and artificial intelligence. He also attended a hearing before the Parliamentary Assembly's Committee on Culture, Science, Education and Media on monitoring and tracing apps deployed in connection with the COVID-19 pandemic.[41]

The DPC made recommendations on the question of data anonymisation and the protection of personal data in judicial proceedings to the Registrar of the Administrative Tribunal. He was asked for an opinion on the lawfulness of the disclosure of data in connection with an internal fraud investigation and consulted on updating the internal regulations regarding protection of personal data. The new Council of Europe Regulations on the Protection of Personal Data were adopted on 15 June 2022.[42]

d) European Data Protection Supervisor

The European Data Protection Supervisor ("**EDPS**") is the independent data protection authority within the European Union responsible for supervising the processing of personal data by the institutions, bodies, offices and agencies of the European Union.[43]

Its powers are set out in Regulation 2018/1725, under which, for example, it may impose administrative fines on EU institutions or refer a case to the CJEU. The EDPS has specific powers to supervise the manner in which certain bodies and agencies process personal data; for example, European Union Agency for Law Enforcement Cooperation (Europol) and the European Public Prosecutor's Office.[44]

[40] Council of Europe, Activity Report of the Data Protection Commissioner: November 2020-October 2022, DPCOM Report 2020-2022, p.5.

[41] Council of Europe, Activity Report of the Data Protection Commissioner: November 2020-October 2022, DPCOM Report 2020-2022, p.7.

[42] Council of Europe, Activity Report of the Data Protection Commissioner: November 2020-October 2022, DPCOM Report 2020-2022, pp. 10 and 12.

[43] European Data Protection Supervisor, Annual Report Executive Summary '22, p.3.

[44] European Data Protection Supervisor, Annual Report Executive Summary '22, pp.4-5.

In addition to monitoring the processing of personal data to ensure compliance with data protection rules, the EDPS:

- advises the European Commission, European Parliament and the Council on legislative proposals and initiatives relating to data protection;
- monitors and assesses technological developments impacting the protection of personal data; and
- works with data protection authorities to promote consistent data protection across the EU.[45]

In 2022, the EDPS had various ongoing investigations into the institutions and agencies of the EU on their use of products and cloud services from entities based outside the European Economic Area, including the European Commission's use of Microsoft Office 365.[46] It also requested that the CJEU annuls certain provisions of the amended Europol Regulation as they undermine legal certainty for individuals' personal data and threaten the independence of the EDPS.

In conjunction with the European Data Protection Board, the EDPS issued a Joint Opinion on the Proposal for the European Health Data Space – the first of a series of proposal for domain-specific common European data spaces – and a Joint Opinion on the Proposal for the Data Act, which aims to establish harmonised rules on the access to, and use of, data generated from a broad range of products and services, such as connected objects and virtual assistants.[47]

[45] European Data Protection Supervisor, Annual Report Executive Summary '22, p.4.

[46] European Data Protection Supervisor, Annual Report Executive Summary '22, p.13.

[47] European Data Protection Supervisor, Annual Report Executive Summary '22, p.16.

Chapter 2

What is private information and personal data?

The protection of personal data is of fundamental importance to a person's enjoyment of the right to respect for private and family life, home and correspondence, as guaranteed by Article 8 ECHR.[48] The collection, storage, alteration, disclosure, use and publication of information relating to an individual's private life can, therefore, represent an interference with Article 8 ECHR.[49]

The Court defines "information relating to an individual's private life", by reference to the definition of personal data in Convention 108.[50] Article 2(a) of Convention 108 provides:

> *"personal data" means any information relating to an identified or identifiable individual ("data subject");[51]*

This definition of personal data must not be interpreted restrictively. It is a broad concept[52] which includes both information which directly identifies an individual (such as their name), as well as information which can be used to identify them indirectly by reference to an identifier such as location data or their internet protocol (IP) address.

---

[48] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, Grand Chamber judgment of 27 June 2017, no. 931/13 at §137.

[49] *Rotaru v. Romania*, Grand Chamber judgment of 4 May 2000, no. 28341/95 at §46.

[50] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108), which entered into force in 1985 and was updated in 2018.

[51] *Amann v. Switzerland*, Grand Chamber judgment of 16 February 2000, no. 27798/95 at §65; *Rotaru v. Romania*, Grand Chamber judgment of 4 May 2000, no. 28341/95 at §43.

[52] *Rotaru v. Romania*, Grand Chamber judgment of 4 May 2000, no. 28341/95 at §43.

The concept of personal data has been found by the Court to include the following types of information (this list is not exhaustive):

- A person's first name and their surname[53]
- A person's date of birth[54]
- A person's home address[55]
- Telephone numbers dialled, telephone, email and Internet usage, such as the date, time, duration of communications[56]
- Messages sent on online messaging services[57]
- A person's dynamic Internet Protocol ("**IP**") address which reveals details such as a person's broader location and the Internet Service Provider ("**ISP**") to which the user is connected (even where they are not named as the subscriber to the ISP)[58]
- Genetic and biometric data, including cellular samples, DNA profiles,[59] fingerprints[60] and voice samples[61]
- Health data, for example information on HIV diagnosis,[62] pregnancy[63] and the carrying out of an abortion[64], mental health and compulsory placement in a mental health facility[65]
- Information on a person's sexual orientation and / or their sex life[66]

---

[53] *Guillot v. France*, judgment of 24 October 1996, no. 22500/93.

[54] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15.

[55] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15.

[56] *Copland v. the United Kingdom*, judgment of 3 April 2007, no. 62617/00 at §§41 and 43.

[57] *Bărbulescu v. Romania*, Grand Chamber judgment of 5 September 2017, no. 61496/08 at §§18 and 74-81.

[58] *Benedik v. Slovenia*, judgment of 24 April 2018, no. 62357/14, §§107-108, where the applicant was found to be 'identifiable' (rather than identified) by his dynamic IP address. The IP address showed that he was connected to a certain ISP, but it was his father who was named as the subscriber. Even though the IP address did not reveal his name or address, the information obtained (location, usage etc.) made him identifiable.

[59] *Trajkovski and Chipovski v. North Macedonia*, judgment of 13 February 2020, nos. 53205/13 and 63320/13; *Boljević v. Serbia*, judgment of 16 June 2020, no. 47443/14.

[60] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 at §§70- 77 and 84 (included as a summary in this publication).

[61] *P.G. and J.H. v. the United Kingdom*, judgment of 25 September 2001, no. 44787/98 at §§38 and 63.

[62] *Z v. Finland*, judgment of 25 February 1997, no. 22009/93 at §§113-114.

[63] *Konovalova v. Russia*, judgment of 9 October 2014, no. 37873/04 at §§39-50.

[64] *M.S. v. Sweden*, judgment of 27 August 1997, no. 20837/92 at §§41-42.

[65] *Malanicheva v. Russia* (dec.), decision of 31 May 2016, no. 50405/06 at §§13 and 15-18.

[66] *Dudgeon v. the United Kingdom*, judgment of 22 October 1981, no. 7525/76 at §41.

- A person's occupation[67]
- GPS location data[68]
- A person's financial situation, financial transactions or professional dealings[69]
- Details of taxable earned and unearned income and taxable net assets[70]
- Information on engagement in political activities and protests[71]
- Political opinions, religious, philosophical and other beliefs[72]
- Membership of associations or trade unions[73]
- Information on criminal offences, proceedings, convictions, cautions or related preventive measures (such as being detained in a police station)[74]
- Ethnic origin[75]

Personal Data in the Public Domain

Even where information is already in the public domain, or can be accessed by the public, it can still be deemed to be "personal data" which merits the protection of Article 8. Whether or not personal data available in the public domain engages the protection of Article 8 will depend on the circumstances of the case, including how the data is collected, used and stored. For example, even where information on a person's taxable income and assets could be accessed by the public, disclosure of this information engaged Article 8 where it was systematically collected and published in a newspaper.[76] Similarly, data on a person's criminal conviction is often available in the public domain; their criminal trial is likely to be open to the public and reported in the media and their conviction stored in a central record

[67] *Khelili v. Switzerland*, judgment of 18 October 2011, no. 16188/07 at §56.

[68] *Uzun v. Germany*, judgment of 2 September 2010, no. 35623/05 at §§49-53.

[69] *M.N. and Others v. San Marino*, judgment of 7 July 2015, no. 28005/12 at §51.

[70] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, Grand Chamber judgment of 27 June 2017, no. 931/13.

[71] *Rotaru v. Romania*, Grand Chamber judgment of 4 May 2000, no. 28341/95 at §44.

[72] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15, §112; *Sinan Işık v. Turkey*, judgment of 2 February 2010, no. 21924/05 at §37.

[73] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §112.

[74] *M.M. v. the United Kingdom*, judgment of 13 November 2012, no. 24029/07 at §188.

[75] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 at §71 (included as a summary in this publication).

[76] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, Grand Chamber judgment of 27 June 2017, no. 931/13.

where it is available for disclosure on request. However, as time passes from the date of the conviction and it fades from the public conscience, data on the conviction increasingly becomes a part of the person's private life. The more time that has passed since a conviction, the greater the emphasis on protecting the privacy of this information.[77]

Sensitive Information and Special Categories of Personal Data

Convention 108 distinguishes certain "Special Categories of Data" which should be afforded greater protection. Article 6 of Convention 108 provides:

> *"Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."*

Convention 108+ added further types of data to the definition of "Special Categories of Data", including genetic and biometric data, trade-union membership, data relating to offences and criminal proceedings in addition to data related to criminal convictions and data revealing ethnic as well as racial origin. Article 6 of Convention 108+ provides:

> *"1. The processing of: – genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures; – biometric data uniquely identifying a person; – personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.*
>
> *2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."*

The Court also treats these categories of data as "sensitive" forms of data which warrant a heightened degree of protection. Such heightened protection is

[77] *M.M. v. the United Kingdom*, judgment of 13 November 2012, no. 24029/07.

in recognition of the fact that the disclosure of such data could dramatically affect a person's private and family life, social and employment situation, or expose them to the risk of ostracization.[78]

[78] *Z v. Finland*, judgment of 25 February 1997, no. 22009/93.

Chapter 3

The protection of private information during the investigative phase of proceedings

There are a number of contexts in which State authorities might seek to collect personal data, for example as part of attempts to combat crime, and to collect evidence for use in prosecutorial and judicial proceedings. The collection of personal data in these contexts can, in certain circumstances, constitute an interference with the right to respect for private and family life, home and correspondence under Article 8.

Once it is demonstrated that Article 8 is engaged, the collection of personal data in this context will constitute a breach of Article 8 unless States can show that the collection and storage of data: (i) pursues a legitimate aim; and (ii) is a proportionate means of achieving such aim. The existence and effective implementation of adequate guarantees against the abuse of data collection powers is one essential aspect of showing that surveillance and the collection of data in this context is carried out only to the extent necessary to pursue a legitimate aim. Each of these factors is discussed in more detail below.

a) Special Investigative Measures

What constitutes an interference with Article 8?

A number of factors are relevant to determining whether a person's privacy is affected by surveillance and investigative measures implemented in public places or in respect of public communications. In some circumstances, people knowingly or intentionally engage in activities that are or can be publicly recorded

or reported, for example when entering an area subject to CCTV surveillance watched by a security guard. It is, therefore, relevant to consider the extent to which a person can reasonably expect their privacy to be protected in any given scenario, to determine whether Article 8 is engaged.[79]

The following are examples of measures that constitute an interference with Art 8:

i) Storage of personal data

The storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8.[80] This applies even where the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons.[81]

ii) Search and Seizure of Personal Data and Correspondence

The search of an individual's home, and the search and seizure of their personal electronic devices, personal files and correspondence engage the right to private and family life, home and correspondence under Article 8. [82] The concept of "home" under Article 8 is not limited to a private individual's home and also includes the registered office of a company or other business premises. The search of a company's premises,[83] the search and seizure of a company's electronic data or files, or the imposition of an order on a company to provide access to and allow

[79] *Herbecq and Association "Ligue des droits de l'homme' v. Belgium*, nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, Decisions and Reports (DR) 92-B, p.92 recording of the visual data collected; *Perry v. the United Kingdom*, judgment of 17 July 2003, no. 63737/00 at §37. On the other hand, creating a systematic or permanent record of such public domain material may give rise to privacy considerations. (*P.G. and J.H. v. the United Kingdom*, judgment of 25 September 2001, no. 44787/98, §57; *Peck v. the United Kingdom*, judgment of 28 January 2003, no. 44647/98 at §§58-59; and *Perry v. the United Kingdom*, judgment of 17 July 2003, no. 63737/00 at §38.)

[80] *Leander v. Sweden*, judgment of 26 March 1987, no. 9248/81 at §48.

[81] *Amann v. Switzerland*, Grand Chamber judgment of 16 February 2000, no. 27798/9 at §69; *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 at §§67 and 75 (included as a summary in this publication).

[82] *Trabajo Rueda v. Spain*, judgment of 30 May 2017, no. 32600/12 at §§44-47; *K.S. and M.S. v. Germany*, judgment of 6 June 2016, no. 3369/11.

[83] *Société Colas Est and Others v. France*, judgment of 16 April 2002, no. 37971/97 at §§40-42 (included as a summary in this publication).

the authorities to make a copy of all data used on its company server[84] engage, therefore, the right to respect for home and correspondence under Article 8.

iii) Secret Surveillance

There are numerous methods of covert surveillance employed by state authorities which can interfere with Article 8. This includes:

- **Telephone tapping**: where a person's calls are intercepted, monitored, transcribed and/or recorded, revealing the content of the calls as they happen.[85] This includes situations where it is a third party's telephone line which has been tapped. [86]
- **Telephone metering**: which involves the disclosure of telephone numbers called, as well as the time and duration of each call. [87]
- **Audio and video surveillance**: which includes the recording of a conversation using a covert device planted on a person, recording voices at a police station, covert CCTV video surveillance at a police station and the installation of a listening device in a person's home or private premises.[88]
- **Geolocation surveillance**: where a GPS device is used (for example the installation of a GPS device on a vehicle) to provide real-time information on a person's location and movements.[89]

iv) Bulk Interception vs Targeted Interception

Bulk interception of communications can be distinguished from targeted interception of communications, both in terms of the nature of the interference with Article 8, and the ways in which States must regulate each type of interference.

[84] *Bernh Larsen Holding AS and Others v. Norway*, judgment of 14 March 2013, no. 24117/08 where the order was deemed to engage the rights to respect for the home and correspondence of the applicant companies.

[85] *Klass and Others v. Germany*, judgment of 6 September 1978, no. 5029/71 (included as a summary in this publication); *Malone v. the United Kingdom*, judgment of 2 August 1984, no. 8691/79 (included as a summary in this publication).

[86] *Lambert v. France*, judgment of 24 August 1998, no. 23618/94 at §21.

[87] *Malone v. the United Kingdom*, judgment of 2 August 1984, no. 8691/79 (included as a summary in this publication).

[88] *Bykov v. Russia*, Grand Chamber judgment of 10 March 2009, no. 4378/02 (included as a summary in this publication); *Perry v. the United Kingdom*, judgment of 17 July 2003, no. 63737/00; *Heglas v. the Czech Republic*, judgment of 1 March 2007, no. 5935/02 (included as a summary in this publication).

[89] *Uzun v. Germany*, judgment of 2 September 2010, no. 35623/05.

Whilst targeted interception of communications is primarily used for the prevention of crime, bulk interception is often used for foreign intelligence gathering and the identification of new threats, from both known and unknown actors, who might be operating across borders, for example those involved in global terrorism, drug trafficking, human trafficking and cyberattacks.

Taking account of this broader purpose of bulk interception, secrecy regarding its existence and operation is arguably key to its success. However, in this increasingly digital age, the vast majority of communications are in digital form and are transported across global telecommunications networks without any meaningful reference to national borders. This means that bulk surveillance measures have a potentially extraordinarily wide reach both inside and outside the State conducting the surveillance. Whilst there is an emphasis on the need for secrecy to enable bulk interception to target broader threats, the breadth of its scope can also render it significantly more intrusive than targeted interception, demanding greater safeguards surrounding its use.

The Court defines bulk interception as a gradual process, in respect of which the degree of interference with Article 8 grows more intense as the process progresses. It splits the process into the following four stages:[90]

i) The interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications).[91] At this stage, the communications of the largest number of people will be intercepted, many of whom will be of no intelligence interest and who will be filtered out.

[90] *Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 (included as a summary in this publication).

[91] Content data is surrounded by multiple pieces of related communications data. While content data might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Bulk related communications data can be analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and an insight into who a person interacted with (*Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 at §256 (included as a summary in this publication)).

ii) The use of initial, largely automated searching using specific selectors to begin to target individuals using the retained communications/related communications data.
iii) Examination of selected communications/related communications data by analysts.
iv) The subsequent retention of data and use of the "final product", including the sharing of data with third parties such as foreign intelligence services. This is the first time the intercept material is actually used by the intelligence services.

Each one of the above four stages of bulk interception constitutes an interference with Article 8.[92]

v) Infiltration of Encrypted Communications

As the surveillance technology employed by state authorities continues to develop, so too do the communication software and devices used by citizens. EncroChat, Sky ECC and Exclu are three companies that have designed communication tools with the specific aim of protecting private communications from interception. All three systems have, however, been intercepted and dismantled by law enforcement agencies. The data obtained from the systems has been used to inform criminal investigations across numerous jurisdictions, disrupt organised crime and take action to prevent imminent criminal acts. Law enforcement agencies credit the data obtained as leading to hundreds of arrests and the widespread seizure of criminal property. In recognition of this potential to harvest extensive information on the operation of serious and organised crime, the United States Federal Bureau of Investigation ("**FBI**") distributed its own supposedly secure messaging technology, ANOM, to seek to monitor the communications of those involved in criminal activity.

[92] *Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 at §§239–244 (included as a summary in this publication).

Encrypted Communication Software: How does it operate?

EncroChat: EncroChat devices are modified mobile phones (with the camera, GPS and USB port removed and a feature to rapidly wipe the phone's content) which can only be used to communicate with other EncroChat devices. EncroChat software encodes or encrypts messages once sent, as they pass through the central EncroChat server located in France. Messages are then decoded or de-encrypted via the software on the receiving handset and so, in theory, only readable by the intended recipient.

Sky ECC: Many former users of EncroChat switched to use the Sky ECC platform, after EncroChat was dismantled in 2020. Sky ECC supplied phones offering self-destructing and encrypted messages and did not store encrypted messages on its servers, if a message was not read within 48 hours, it could not be retrieved.

ANOM: ANOM is an encrypted device company devised by the FBI. It was distributed amongst criminal groups who sold and promoted the technology worldwide. A copy of every message sent from an ANOM device was sent to a server in a third-party country where the messages were collected, stored and provided to the FBI on a regular basis pursuant to an international cooperation agreement. ANOM, unlike EncroChat and Sky ECC, was exploited by the FBI from the beginning. Data collection from ANOM was not an infiltration of an existing encrypted communications company.

A variety of methods were used to obtain and intercept data from this encrypted communication software. The law enforcement agencies involved in the interception of such encrypted communications, intercepted, shared and analysed millions of messages. For example, in respect of EncroChat, the French police implanted malware on all EncroChat devices which captured all data which had not been erased and all messages which were created thereafter. They were able to read messages in real time.

A significant proportion of the people sending intercepted messages were based outside the countries whose law enforcement agencies were conducting

real-time interception.[93] As such, the data harvested was also shared with investigators across numerous other jurisdictions.[94] This raises two potential interferences with Article 8: i) in respect of the data collection; and ii) in respect of the data transfer across jurisdictions. Given the breadth of the definition of personal data (described above), and the broad range of actions which have so far been deemed to constitute an interference with Article 8 in this context (also described above), it seems likely that both actions will be deemed to constitute an interference with Article 8.

Victim Status

i) Demonstrating victim status

Under Article 34 ECHR an applicant must show that they have been "the victim" of a violation of their ECHR rights, in order to bring a claim to the ECtHR. This provision has been interpreted to mean that the Convention does not allow for applicants to bring claims *in abstracto*. Instead, applicants must generally show that they have been directly affected by the measure complained of.

However, this test is applied with a degree of flexibility in the context of secret surveillance, in light of the particular features of secret surveillance measures. By their very nature, the existence and application of secret surveillance measures can remain unknown to those impacted by them.[95] A strict application of the "victim" status test in this context could, therefore, lead to a situation in which secret surveillance measures become effectively unchallengeable, rendering the protections of Article 8 a nullity, where a person could be treated in a manner contrary to Article 8 without ever knowing about it. A more flexible approach to the "victim" test in this context is important to ensure that such measures remain subject to the supervision and scrutiny of the courts.

[93] European Union Agency for Criminal Justice Cooperation, "New Major interventions to block encrypted communications of criminal networks" (2021) available at https://t.ly/ZTUzn.

[94] Serbia, Bosnia and Herzegovina, Albania, Montenegro and Slovenia, almost 100 people have been arrested and charged as a result of evidence obtained from Sky ECC communications: see Ivana Jeremic et al, "Encrypted Phone Crack No Silver Bullet against Balkan Crime Gangs" (*Balkan Insight*, 25 April 2022) available at https://t.ly/SCBvp; and Europol, "Balkans' biggest drug lords arrested after investigation into encrypted phones" (12 May 2023) available at https://t.ly/1iDtO.

[95] See *Klass and Others v. Germany*, judgment of 6 September 1978, no. 5029/71 at §§34-36 (included as a summary in this publication).

In certain circumstances an applicant can, therefore, claim to be the victim of a violation of their Article 8 rights as a result of the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures. In cases concerning such surveillance measures, the Court has concluded that "*… each of the applicants is entitled to "(claim) to be the victim of a violation" of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance. The question whether the applicants were actually the victims of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions.*"[96]

The following factors are relevant to determining if an applicant can claim victim status:

» **The availability and efficacy of remedies at a national level**: two key scenarios can be distinguished:

  i) Where the national system does not afford effective remedies for a person who suspects that they have been subjected to secret surveillance, this can give rise to widespread suspicion and concern amongst the general public that surveillance powers are being abused. In such circumstances, the threat of surveillance itself can restrict free communication and interfere with the Article 8 rights of all potential users of communication services. An individual in this situation would not need to demonstrate the existence of a risk that secret surveillance measures were applied to them.
  ii) Where the national system provides for effective remedies for those who suspect that they have been subjected to secret surveillance, a more widespread suspicion of abuse of power is more difficult to justify. An individual in this situation would need to show that, due to their personal situation, they are potentially at risk of being subjected to the surveillance measures (see below).

» **The scope of the legislation permitting surveillance measures**: an individual can show that they are at risk of being subjected to surveillance measures in the following situations:

[96] *Klass and Others v. Germany*, judgment of 6 September 1978, no. 5029/71 at §38 (included as a summary in this publication).

i) The person belongs to a group of people targeted by the legislation; or
ii) The legislation institutes a system where any user of a communication system's communications could be intercepted.
iii) Do legal entities have a right to data protection?

EU law data protection rules (under the CFR and the GDPR) apply only to personal data about individuals or "natural persons", they do not govern data about companies or any other legal entities. However, information in relation to one-person companies may constitute personal data where it allows the identification of a natural person.[97]

Similarly, under the ECHR legal entities do not have a right to respect for their private life, *per se*. However, legal entities, including companies, law firms, non-governmental organisations etc. are entitled to rely on Article 8 rights in this context where they are impacted by a measure which breaches their right to respect for their "correspondence" or "home" under Article 8. The concept of "home" under Article 8 includes the registered office of a company or other business premises (see above).[98] The search of a company's premises, the search and seizure of a company's electronic data or files, or the imposition of an order on a company to provide access to and allow the authorities to make a copy of all data used on its company server[99] engage, therefore, the right to respect for home and correspondence under Article 8. Similarly, the surveillance and interception of telephone, email and facsimile communications between the staff of legal entities can interfere with those legal entities' right to respect for correspondence.[100]

Further, both Article 8 ECHR and EU law data protection rules also apply to all personal data relating to natural persons in the course of a professional activity, such as the employees of a company or organisation, including their business email addresses or employees' business telephone numbers.

[97] *Camera di Commercio, Industria, Artigianato e Agrocoltura di Lecce v. Salvatore Manni* C-398/15, CJEU judgment of 9 March 2017.

[98] *Société Colas Est and Others v. France*, judgment of 16 April 2022, no. 37971/97 at §§40-42 (included as a summary in this publication).

[99] *Bernh Larsen Holding AS and Others v. Norway*, judgment of 14 March 2013, no. 24117/08.

[100] *Liberty and Others v. the United Kingdom*, judgment of 1 July 2008, no. 58243/00.

In accordance with law

The requirement for any measure which interferes with Article 8 to be "in accordance with law" means that the measure must have: i) some basis in domestic law; and ii) it must be compatible with the rule of law. This generally means that the law regulating a measure which interferes with Article 8 rights must be accessible to the person concerned and be drafted with sufficient clarity to render it foreseeable as to its effects.[101]

However, this requirement of "foreseeability" must be interpreted slightly differently in the specific context of secret surveillance measures. Because of the need for secrecy surrounding the order and imposition of such measures, foreseeability in this context does not mean that individuals should be able to foresee when the authorities are likely to resort to such measure, so that they can adapt their behaviour accordingly.

Instead, in this context, foreseeability requires States to have in place clear, detailed rules on their use of secret surveillance measures which provide citizens with at least an adequate indication as to the circumstances in which and the conditions under which public authorities are empowered to resort to any such measure.[102] The law authorising the use of such measures must indicate the scope of any discretion conferred on the authorities and the manner of its exercise.[103]

In this context, the "in accordance with law" test, is closely related to the "necessity" test (described below). The legal basis for the measures and the legal regime governing their use must be sufficient to provide adequate and effective safeguards against abuse and to ensure that surveillance measures are employed only when necessary in a democratic society.[104]

---

[101] *Roman Zakharov v. Russia*, Grand Chamber judgment of 4 December 2015, no. 47143/06 at §228 (included as a summary in this publication).

[102] *Roman Zakharov v. Russia*, Grand Chamber judgment of 4 December 2015, no. 47143/06 at §229 (included as a summary in this publication).

[103] *Roman Zakharov v. Russia*, Grand Chamber judgment of 4 December 2015, no. 47143/06 at §230 (included as a summary in this publication).

[104] *Roman Zakharov v. Russia*, Grand Chamber judgment of 4 December 2015, no. 47143/06 at §36 (included as a summary in this publication); *Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 at §248 (included as a summary in this publication).

Pursuit of a legitimate aim

Article 8(2) provides:

> *"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 wellbeing 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."*

Thus, the data search, seizure and storage and the surveillance mechanisms discussed in section (a) above will not breach Article 8, if they are necessary and proportionate means of protecting national security, public safety or preventing disorder or crime. For example, the Court has found that Article 8 does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats.[105] Similarly, in several cases, it has emphasised that States might consider it necessary to have recourse to searches and seizures to obtain physical evidence of offences.[106]

Necessity

In general, States are afforded a wide margin of appreciation to determine how best to achieve the aim of protecting national security, including the question of what type of surveillance or communications interception regime is necessary.[107]

However, in recognition of the serious risk of abuse of power and the potentially broad-ranging interferences with Article 8 rights which can arise from the use of search, seizure and surveillance measures, States must be able to show that they have implemented adequate and effective guarantees against abuse. Any interference with Article 8 rights must only be carried out to the extent "necessary in a democratic society".

---

[105] *Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 at §261 (included as a summary in this publication).

[106] *Vasylchuk v. Ukraine*, judgment of 13 June 2013, no. 24402/07 at §79; *K.S. and M.S. v. Germany*, judgment of 6 October 2016, no. 33696/11 at §43.

[107] *Weber and Saravia v. Germany* (dec.), decision of 29 June 2006, no. 54934/00 at §106; *Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 at §261 (included as a summary in this publication).

When determining whether an interference is necessary in a democratic society, it is necessary to take account of all the circumstances of a case. In particular, the following factors will be relevant:

- The seriousness of the offence investigated and the urgency with which action must be taken to investigate it.
- The nature, scope and duration of the measures.
- The availability of other sources of evidence.
- The nature and scope of the grounds required before ordering such measures.
- The nature of the authorities and systems in place to authorise and carry out the measures.
- The review mechanisms in place to supervise the ordering and implementation of such measures.
- The existence and efficacy of remedies for those who have been or suspect they have been subject to such measures.

Depending on the nature, scope and duration of surveillance measures, different safeguards will be required. For example, a broad-ranging or indiscriminate search is less likely to be justified than a targeted measure, in particular where it is used to investigate a minor offence or where it is conducted in respect of a third party, rather than the accused.[108]

In respect of surveillance measures, two key factors used to assess whether an interference is necessary in a democratic society include: (i) the quality of the legal regime authorising and regulating the use of such measures; and (ii) the availability and efficacy of independent review mechanisms.

i) The legal regime authorising and regulating the use of targeted surveillance measures

As described above, the legal regime authorising and governing the use of secret surveillance measures must ensure that such measures are only employed when it is "necessary in a democratic society".

[108] *Buck v. Germany*, judgment of 28 April 2005, no. 41604/98 at §§30-53.

As a minimum, in order to act as an effective safeguard against the abuse of power, laws regulating the use of targeted secret surveillance powers must set out and provide clarity on the following factors:

i) the nature of offences which may give rise to an interception order;
ii) a definition of the categories of people liable to have their communications intercepted;
iii) a limit on the duration of interception;
iv) the procedure to be followed for examining, using and storing the data obtained;
v) the precautions to be taken when communicating the data to other parties; and
vi) the circumstances in which intercepted data may or must be erased or destroyed.

These requirements apply where targeted surveillance measures are used as part of a criminal investigation, as well as where targeted measures are used for reasons of national security.[109]

ii) Supervision and review of targeted surveillance measures

Review and supervision mechanisms must be implemented at the following three stages of secret surveillance:

i) When the surveillance is first ordered;
ii) While it is being carried out; and
iii) After it has been terminated.

In order to keep surveillance measures secret, stages (i) and (ii) above must be carried out without the knowledge or involvement of the individual who is subject to the measure. It is essential, therefore, to implement a procedure by which supervisory control of the ordering and implementation of secret surveillance is exercised by an independent and impartial supervisory authority. Ideally this should be a judge to provide the best guarantee of independence, impartiality and proper procedure.[110]

[109] *Roman Zakharov v. Russia*, Grand Chamber judgment of 4 December 2015, no. 47143/06 at §231.

[110] *Roman Zakharov v. Russia*, Grand Chamber judgment of 4 December 2015, no. 47143/06 at §233.

The existence of a procedure to notify a person of the measure taken, after surveillance has terminated, will be a key factor to determine the efficacy of review measures at stage (iii). A person must be informed of the measures taken to enable them to challenge their legality retrospectively. If a State does not have a notification procedure, it would at least need to have a system in place to enable a person to bring a claim to domestic courts if they merely suspect they have been the subject of surveillance.

iii) Bulk interception measures

Different considerations apply when examining the necessity of bulk interception measures. As described in section 4(a)(iv) above, bulk interception serves a different purpose and affords States access to a broader scope of information, about a wider range of people.[111] Its use for foreign intelligence gathering might not be targeted at any specific individual, instead sometimes being used to obtain new leads.

Whilst Article 8 does not prohibit the operation of bulk interception systems to protect national security and other essential national interests, States' margin of appreciation is narrower in this context, and the need for safeguards is greater.[112] Additionally, the initial stages of bulk interception often involve automatic processing of data and the need for safeguards is often greater where personal data is subject to automatic processing.[113] The safeguards applied to guard against an abuse of the use of a bulk interception regime must be adapted to take account of its specific features.

The legal regime authorising and regulating bulk interception measures

The minimum safeguards applicable to targeted interception cases, requiring a clear definition of the nature of offences and the categories of people liable to have their communications intercepted, cannot readily be applied in the context of bulk interception.

[111] See section 4(a)(iv) of this publication and in particular footnote 91 above

[112] *Centrum för rättvisa v. Sweden*, Grand Chamber judgment of 25 May 2021, no. 35252/08 at §261 (included as a summary in this publication).

[113] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 at §103 (included as a summary in this publication).

It is, essential, therefore, that States implement domestic laws specifically regulating the use of bulk interception measures. These rules must clearly define:

i) the grounds upon which bulk interception might be authorised;
ii) the circumstances in which an individual's communications might be intercepted;
iii) the procedure to be followed for granting authorisation;
iv) the procedure to be followed for selecting, examining, using and storing the data obtained;
v) the precautions to be taken when communicating the data to other parties;
vi) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased or destroyed;
vii) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and
viii) the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

Supervision and review of bulk interception measures

For reasons of national security, States will often not be at liberty to disclose information on the operation of a bulk interception regime (even retrospectively). This increases the potential for abuse and amplifies the importance of effective mechanisms for supervision and review. Authorisation and oversight of the process are, therefore, the most significant safeguards of Article 8 compliance.

Bulk interception regimes must be subject to the following end-to-end safeguards:

i) Independent authorisation at the outset, evaluating the necessity and proportionality of the object and scope of the operation.
   a) Judicial authorisation is a preferable but not necessary, so long as authorisation is carried out by an independent body.
   b) The independent authorising body must be informed of the purpose of the interception and the bearers or communication routes likely to be intercepted.

c) It is not necessary to include all the "selectors" that will be used in the authorisation request, but it should at least identify the types of categories of selectors that will be used.

ii) Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material should also be subject to robust supervision by an independent authority to keep the "interference" to what is "necessary in a democratic society".

iii) Enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified – with regard to the principles of necessity and proportionality.

iv) Detailed records should be kept by the intelligence services at each stage of the process to facilitate supervision and review.

v) Ex-post facto review mechanisms must be in place:
   a) Given that a notification requirement is unlikely to be implemented in this context, an effective remedy must be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime.
   b) The remedy must be before a body / authority which is independent of the executive and offers, so far as possible, an adversarial process to assess the overall fairness of regime and, primarily, whether the domestic legal framework complies with the eight requirements set out above.

Transfer of intercept material to third parties

The transmission of bulk interception material by one State to another State or to an international organisation should be limited to material that has been collected and stored in a Convention compliant manner and the transfer should be subject to certain additional safeguards:

i) The circumstances in which a transfer can take place must be set out clearly in domestic law.

ii) The transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference when handling the data,

to guarantee its secure storage and restrict onward disclosure.

iii) Heightened safeguards will be necessary when transferring material requiring special confidentiality – such as confidential journalistic material.

iv) The transfer of material to foreign intelligence partners should be subject to independent control.

Application to encrypted communications interception

It is not yet clear whether or not the collection, storage and transfer of data obtained from EncroChat, Anom, and Sky ECC will constitute a breach of Article 8. For example, in respect of EncroChat, it is likely to be relevant that the French judiciary authorised the measures in advance on the basis they were necessary to identify and arrest users implicated in illegal activities. However French lawyers have challenged the absence of a time limitation on interception measures in these court orders, the massive and indiscriminate nature of the measures authorised and the fact that arguable, the measures authorised go beyond the actions which can be justified by their envisaged legal bases.[114]

b) The use of material obtained in breach of Article 8 in judicial proceedings

Whilst the investigative measures discussed above might give rise to a breach of Article 8, individuals impacted by such measures might also seek to challenge their use as evidence in judicial proceedings, on the basis of a breach of their Article 6 right to a fair hearing. However, simply because evidence has been obtained in breach of Article 8, does not necessarily mean it will be deemed inadmissible in judicial proceedings, and its use in such proceedings will not automatically give rise to a breach of Article 6.

Article 6 ECHR guarantees the right to a fair hearing, but it does not lay down any specific rules on the admissibility of evidence. The design of rules on admissibility of evidence is primarily a matter for domestic law. The Court has consistently reiterated that it is not its role to determine, as a matter of principle, whether certain types of evidence are admissible.[115]

[114] European Parliament, "At a glance: EncroChat's path to Europe's highest courts", available at https://t.ly/iineP.

[115] *Khan v. the United Kingdom*, judgment of 12 May 2000, no. 35394/97 (included as a summary in this publication); *Allan v. the United Kingdom*, judgment of 5 November 2002, no. 48539/99; *Heglas v. the Czech Republic*, judgment of 1 March 2007, no. 5935/02 (included as a summary in this publication); *Dragojevic v.*

Instead, the key question when assessing compliance with Article 6 is whether proceedings as a whole are fair, taking account of all the circumstances of the case, including the way evidence has been obtained and admitted to proceedings. The admission of evidence obtained in breach of Article 8 is, therefore, one of numerous factors that should be taken into account when determining if proceedings are fair. In criminal, administrative[116] and civil proceedings,[117] evidence obtained in breach of Article 8 can be admitted without breaching the right to a fair hearing under Article 6 without necessarily compromising the fairness of proceedings as a whole. For example, evidence and information obtained via phone tapping,[118] or covert listening and recording devices[119] in breach of Article 8, does not necessarily breach Article 6 if it is relied upon in a criminal trial.

When assessing whether or not proceedings as a whole are fair (and so whether or not they are Article 6 compliant), it is necessary to take account of the following factors:

- The nature of the unlawfulness in question and the nature of the violation of Article 8.
- Whether or not the applicant was given the opportunity to challenge the authenticity of the evidence and to oppose its use.
- Whether or not fair procedures were in place to challenge the admissibility of evidence, in particular, an adversarial process.
- The extent to which objections to the admissibility of such materials are examined and addressed by courts and the extent to which courts provide reasoned decisions for allowing the evidence to be admitted.
- The quality of the evidence, and the extent to which the circumstances in which it was obtained cast doubt on its reliability or accuracy.
- The existence of any safeguards in place to guarantee or assess the reliability of the evidence. For example, calling independent experts as witnesses to analyse and explain the evidence and / or producing and admitting evidence

Croatia, judgment of 15 January 2015, no. 68955/11 (included as a summary in this publication); *Bykov v. Russia*, Grand Chamber judgment of 10 March 2009, no. 4378/02 (included as a summary in this publication).

[116] *Vukota-Bojic v. Switzerland*, judgment of 18 October 2016, no. 61838/10 at §77.

[117] *Bărbulescu v. Romania*, Grand Chamber judgment of 5 September 2017, no. 61496/08 at §§140-141.

[118] *Dragojevic v. Croatia*, judgment of 15 January 2015, no. 68955/11 (included as a summary in this publication).

[119] *Khan v. the United Kingdom*, judgment of 12 May 2000, no. 35394/97 (included as a summary in this publication).

independent and expert reports analysing the evidence.[120]

- » The availability of other evidence and the extent to which the conviction is based on a range of sources of evidence, e.g. witness statements and evidence obtained through search and seizures, in addition to evidence obtained via covert surveillance.[121]
- » The extent to which an important public interest is served by admitting evidence obtained in breach of Article 8, for example if it is used to investigate, convict and punish a serious criminal offence.[122]

The extent to which other, supporting evidence is required depends on the strength and authenticity of the unlawfully obtained evidence. Where unlawfully obtained evidence is very strong, and there is no risk of it being unreliable, the need for supporting evidence is correspondingly weaker.[123]

It is, however, important to examine whether evidence obtained via surveillance or interception provides access to conversations and information which have been provided freely and spontaneously, or whether the relevant individual has been pressured or coerced into making certain statements or admissions. Where recorded or intercepted evidence is obtained via coercion or oppression, its admission would breach Article 6(1) if the pressure imposed has impacted the voluntary nature of the admissions to the extent that it could be regarded as having impinged on the person's right to remain silent and the privilege against self-incrimination.[124] For example, where the nature of a recorded conversation could be regarded as the functional equivalent of interrogation, but has taken place without any of the safeguards which would normally attach to a formal police interview, such as a caution or the presence of legal support.[125]

---

[120] *Bykov v. Russia*, Grand Chamber judgment of 10 March 2009, no. 4378/02 at §§37 and 103 (included as a summary in this publication).

[121] *Dragojević v. Croatia*, judgment of 15 January 2015, no. 68955/11 at §§133-134 (included as a summary in this publication).

[122] *Heglas v. the Czech Republic*, judgment of 1 March 2007, no. 5935/02 at §§90-91 (included as a summary in this publication).

[123] *Khan v. the United Kingdom*, judgment of 12 May 2000, no. 35394/97 at §§35 and 37 (included as a summary in this publication); and *Allan v. the United Kingdom*, judgment of 5 November 2002, no. 48539/99 at §43.

[124] *Bykov v. Russia*, Grand Chamber judgment of 10 March 2009, no. 4378/02 at §§100-102 (included as a summary in this publication), which contrasts *Allan v. the United Kingdom*, judgment of 5 November 2002, no. 48539/99, where a breach of Article 6 was found, with *Heglas v. the Czech Republic*, judgment of 1 March 2007, no. 5935/02 (included as a summary in this publication), where Article 6 was not found to have been breached.

[125] *Allan v. the United Kingdom*, judgment of 5 November 2002, no. 48539/99 at §§45-53.

Admissibility of intercepted encrypted communications

As evidence obtained from the interception of EncroChat, Sky ECC and ANOM devices has now been used to investigate and prosecute 1000s of people across Europe, complaints have been brought regarding the admission of such material as evidence in criminal trials. Neither the ECtHR or the CJEU has yet determined a case regarding the impact of admitting such evidence on the right to a fair hearing under Article 6.[126] However, the principles above continue to be relevant and a case-by-case analysis of the overall fairness of proceedings will be required.

In the specific context of evidence obtained through EncroChat, Sky ECC, and ANOM one of the key factors that is likely to be relevant is the extent to which the defence is able to challenge and examine the authenticity and reliability of the evidence.[127] Interception of EncroChat, Sky ECC and ANOM devices relies on innovative and cross-border technology. The efficacy of such technology to assist in investigating and countering crime in part relies upon maintaining secrecy surrounding how it is developed and used, so as not to enable criminal networks to develop means to counter such interception. As such, state authorities are often unwilling to disclose detailed technical information regarding how data has been obtained, analysed, processed and transferred.[128] Without this knowledge, it can become almost impossible for defendants to challenge the authenticity and legitimacy of the evidence.[129] This is despite the possibility that there may have

[126] The Berlin Regional Court has requested a preliminary ruling from the Court of Justice of the European Union ("**CJEU**") on 14 critical questions concerning the use of evidence obtained from EncroChat. The questions raised include whether the German investigating authorities breached EU Law when obtaining the data, and if so, do such infringements of EU law mean that the data cannot be used as evidence in criminal proceedings. See: Request for a preliminary ruling from the Landgericht Berlin (Germany) lodged on 24 October 2022 — *Criminal proceedings against M.N.* (Case C-670/22).

[127] For example, the Italian Supreme Court ruled that encrypted messages obtained by an international police operation to hack a second phone network used by organised crime groups cannot be used in a pre-trial hearing unless prosecutors explain how the evidence was obtained. Italy's Corte di Cassazione found that a defendant should not only have the ability to ask questions about the contents of messages police obtained from the Sky ECC phone network, but also to question how the investigative process was carried out: European Parliament, "At a glance: EncroChat's path to Europe's highest courts", available at https://t.ly/iineP.

[128] For example, the French Gendarmerie have been unwilling to disclose technical details of the EncroChat investigation: European Parliament, "At a glance: EncroChat's path to Europe's highest courts", available at https://t.ly/iineP.

[129] In two open letters, more than 100 Dutch defence lawyers and 22 European lawyers practising criminal law,

been defects in the technology used, mistakes made in the analysis of the data and a risk that raw data can be manipulated.[130]

Where limited data is provided regarding the process to obtain and analyse this kind of intercept material, it is likely that the existence of other evidence to secure a conviction will be a key factor to determine if proceedings as a whole are fair. For example, a defendant who was first identified through EncroChat evidence, but was subsequently found in possession of illicit weapons or drugs, is less likely to be able to challenge the fairness of proceedings where his conviction is based on evidence consisting of EncroChat evidence in addition to evidence obtained through a subsequent search and seizure. By contrast, someone whose conviction is based on EncroChat data alone may have a stronger basis to challenge the fairness of proceedings. Independent technological experts, with experience of the technology used, might also play a key role, where they are involved to analyse and explain the authenticity of evidence, or express any potential doubts about its legitimacy.

Further, an enormous amount of the intercepted data has been obtained in one country but transferred for use by the investigating authorities in another. Whilst the design of rules surrounding admissibility of evidence is a task for national authorities, rather than the ECtHR, the ECtHR will supervise compliance with Article 8 and Article 6 by assessing whether evidence has been obtained, and hearings proceeded, in accordance with the law or "according to law". National authorities must, therefore, ensure that proceedings take place, and evidence is admitted in a manner which is foreseeable and complies with their domestic laws. This can be harder to ensure where evidence is gathered in another jurisdiction, whose laws and safeguards surrounding gathering evidence may be different to those in which the evidence is being admitted to trials. Domestic courts must, however, apply their domestic rules to assess whether or not the data obtained abroad is admissible.

---

respectively, many directly involved in defending EncroChat users, criticised the fact that defendants face unfair trials because prosecutors refuse to disclose information about the hacking operations: Bill Goodwin, "Dutch lawyers raise human rights concerns over hacked cryptophone data" (*ComputerWeekly.com*, October 2022) available at https://t.ly/UOGVi and Fair Trials, "EncroChat hack: Fair Trials denounces lack of transparency and oversight" (February 2022) available at https://t.ly/n1BYX.

[130] Ivana Jeremic et al, "Encrypted Phone Crack No Silver Bullet against Balkan Crime Gangs" (*Balkan Insight*, 25 April 2022) available at https://t.ly/SCBvp - in which Professor Dennis-Kenji Kipker, a board member at the European Academy for Freedom of Information and Data Protection, EAID states: "When the raw data, digital data is being used, it can be changed and the data authenticity and the data integrity cannot be guaranteed."

Chapter 4

Publication of information during judicial proceedings

In addition to the ways in which admitting evidence obtained in breach of Article 8 might impact on the overall fairness of proceedings (as discussed earlier in this guide), there are numerous other ways in which the specific guarantees provided by Article 6 interact with and might be impacted by the requirements to protect personal data under Article 8. For example, where information about a suspect is published during an investigation, this might impact on the right to be presumed innocent until proven guilty. Further, where personal data forms part of the evidence presented during a hearing, it is necessary to balance, on the one hand, the protection of the public nature of judicial proceedings, which is necessary to uphold trust in the courts, and, on the other hand, the interests of a party or of a third person in maintaining the confidentiality of his or her data.

During the investigative stage of judicial proceedings there are two key ways in which Convention rights might be engaged when information is shared with the public about those proceedings. In the specific context of criminal proceedings, public statements made prior to the conclusion of a criminal trial have the potential to breach the right to be presumed innocent, protected under Article 6(2) ECHR, where such statements include premature assertions that the accused is guilty.

In addition, there may be contexts in which personal information is shared about those involved in ongoing judicial proceedings, where Article 6(2) is not engaged, but Article 8 is. For example, the publication of a photograph of an accused, or a party in the context of civil, rather than criminal proceedings, where Article 6(2) does not apply.

a) The right to be presumed innocent until proved guilty under Article 6

Article 6(2) ECHR provides that:

> *"Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law."*

This provision requires that members of the court should not start a criminal hearing with the pre-conceived idea that the accused has committed the offence of which they are charged. It imposes requirements in respect of (amongst other things) any publicity or statements made pre-trial by public officials. Any such statements or publicity must be drafted and delivered carefully to ensure that they do not include premature expressions or assertion of a person's guilt, to avoid interfering with their right to be presumed innocent.

i) Who does Article 6(2) apply to?

The obligation to avoid making statements which undermine the presumption of innocence applies to all public authorities. It prohibits, therefore, the premature expression by a judge, tribunal or members of the court that a person charged with a criminal offence is guilty, before the conclusion of their trial. It also prohibits statements made by any other public officials about pending criminal investigations which encourage the public to believe a suspect is guilty and so prejudge the assessment of the facts by the competent judicial authority. [131] In this respect, the requirements of Article 6(2) extend to the president, prime minister, politicians, government ministers, prosecutors and the police of a State and could arise, for example, when public officials make statements as part of a newspaper or television interview, or when they deliver a press-conference.[132]

When the impugned statements are made by private entities (such as newspapers), and do not constitute a verbatim reproduction of (or an otherwise direct quotation from) any part of official information provided by the authorities, an issue does not arise under Article 6(2). However, an issue might arise under Article 8 ECHR (see below).[133]

[131] *Allenet de Ribemont v. France*, judgment of 10 February 1995, no. 15175/89 at §36.

[132] *Peša v. Croatia*, judgment of 8 April 2010, no. 40523/08 at §§138 and 141.

[133] *Mityanin and Leonov v. Russia*, judgment of 7 May 2019, nos. 11436/06 and 22912/06 at §§102 and 105.

ii) When does Article 6(2) apply?

The requirements of Article 6(2) apply to criminal proceedings in their entirety. Normally, the protection of Article 6(2) is triggered as soon as a criminal charge is initiated against a person, i.e. when they are officially notified by the competent authority of an allegation that they have committed a criminal offence.[134] It continues to apply throughout proceedings, through to the conclusion of any final appeal rights. For example, Article 6(2) does not cease to apply solely because first-instance proceedings resulted in a conviction, if that decision is subject to an ongoing appeal.[135]

iii) What does Article 6(2) require?

Article 6(2) does not prevent public authorities from informing the public about criminal investigations in progress. The right to freedom of expression under Article 10 ECHR, which includes the right to receive and impart information, protects the right for the public to receive, and public authorities to impart, information about ongoing criminal investigations.[136] In particular, where criminal proceedings are of significant public importance or public interest, state authorities might be required to keep the public informed of the alleged offence and related criminal proceedings. For example, where criminal proceedings concern allegations of misconduct in office by a high-profile political figure.[137]

Any public statements about ongoing criminal proceedings must, however, be made with the discretion and circumspection necessary to respect the presumption of innocence.[138] Public officials are permitted to make factual statements that someone is merely suspected of having committed a crime and

[134] *Gogitidze and Others v. Georgia*, judgment of 12 May 2015, no. 36862/05 at §§125-126; although, see by contrast, *Batiashvili v. Georgia*, judgment of 10 October 2019, no. 8284/07 at §79, where Article 6(2) exceptionally applied from the moment that the authorities manipulated an audio recording and disseminated it to the public to insinuate the existence of a crime, where charges were formally brought against the applicant four days later.

[135] *Konstas v. Greece*, judgment of 24 May 2011, no. 53466/07 at §36.

[136] *Allenet de Ribemont v. France*, judgment of 10 February 1995, no. 15175/89 at §38; *Daktaras v. Lithuania* (dec.), decision of 11 January 2000, no. 42095/98 at §41; *Gutsanovi v. Bulgaria*, judgment of 15 October 2013, no. 34529/10 (included as a summary in this publication).

[137] *Arrigo and Vella v. Malta* (dec.), decision of 10 May 2005, no. 6569/04; *Algirdas Butkevičius v. Lithuania*, judgment of 14 June 2022, no. 70489/17 at §51 (included as a summary in this publication).

[138] *Allenet de Ribemont v. France*, judgment of 10 February 1995, no. 15175/89 at §38.

can provide objective updates on the status of an ongoing investigation. For example, the following are all statements that can be made, and information that can be provided, in compliance with Article 6(2):[139]

- A statement that someone has been arrested and detained pending further investigation;
- Explaining that a criminal case has been opened;
- Reading out a statement of charges;
- Explaining the nature of the charges and possible sentences; and
- Describing the investigative measures taken so far, such as stating that a search has been carried out.

However, to avoid infringing Article 6(2), public officials must not make statements which declare that an individual has committed the crime in question. They must not express opinions that amount to a declaration of the person's guilt or which encourage the public to believe them to be guilty and so which can prejudice the assessment of the facts by a judicial authority.[140]

In this context, the choice of words used by public authorities is of fundamental importance. To assess whether Article 6(2) has been breached, it is necessary to take account of all the circumstances of a case, including how a public statement has been phrased, the particular wording used and the context in which the statements are made.[141]

Statements made must not go beyond the mere conveying of information. For example, officials should avoid the use of language which unequivocally states that the accused has carried out the actions of which they are accused, or which describes them as carrying our such actions. This includes the use of the phrases such as "*what they have done represents an elaborate conspiracy*" to unequivocally indicate that criminal operations have been carried out by the accused,[142] the use

[139] *Gutsanovi v. Bulgaria*, judgment of 15 October 2013, no. 34529/10 at §197 (included as a summary in this publication).

[140] *Algirdas Butkevičius v. Lithuania*, judgment of 14 June 2022, no. 70489/17 at §53 (included as a summary in this publication); *Gutsanovi v. Bulgaria*, judgment of 15 October 2013, no. 34529/10 (included as a summary in this publication); *Garycki v. Poland*, judgment of 6 February 2007, no. 14348/02 at §67.

[141] *Daktaras v. Lithuania* (dec.), decision of 11 January 2000, no. 42095/98 at §§41-42.

[142] *Gutsanovi v. Bulgaria*, judgment of 15 October 2013, no. 34529/10 at §200 (included as a summary in this publication).

of phrases such as "*I have no doubt*" that the accused carried out the offence, or describing the accused of being a "*bribe-taker*" before there is evidence they have taken a bribe[143] and sharing photos of suspects referring to them as "*members of the illegal organisation*".[144]

Other relevant factors, in addition to the wording of any statements, include the timing of any statements, which are more likely to infringe Article 6(2) if they are made at a time of high public interest in a case, for example, immediately after a person's arrest or shortly before they appear at their trial.[145] The extent of the media coverage of the statements and the status, position and level of authority of the person making the statement are also relevant.[146] The absence of an intention to undermine the presumption of innocence is irrelevant in this assessment.

b) The publication of information concerning ongoing proceedings - protection under Article 8

As explained above, Article 6(2) cannot prevent the authorities from informing the public about ongoing criminal investigations. Under Article 6(2), personal information can be shared and a suspect's photograph can be published without violating the presumption of innocence, so long as the information and photographs are shared without any assessment or pre-judgment of guilt.[147] However, even where Article 6(2) is not engaged, the publication of such data can amount to an interference with Article 8. To avoid breaching Article 8, the publication of such personal data must be carried out in accordance with law, pursue a legitimate aim, and be deemed to be a proportionate means to achieve that legitimate aim.

[143] *Algirdas Butkevičius v. Lithuania*, judgment of 14 June 2022, no. 70489/17 at §§52-53 (included as a summary in this publication).

[144] *Y.B. and Others v. Turkey*, judgment of 28 October 2004, nos. 48173/99 and 48319/99.

[145] *Algirdas Butkevičius v. Lithuania*, judgment of 14 June 2022, no. 70489/17 at §51(included as a summary in this publication).

[146] *Gutsanovi v. Bulgaria*, judgment of 15 October 2013, no. 34529/10 at §§199-201 (included as a summary in this publication); *Algirdas Butkevičius v. Lithuania*, judgment of 14 June 2022, no. 70489/17 at §§50-53 (included as a summary in this publication).

[147] *Y.B. and Others v. Turkey*, judgment of 28 October 2004, nos. 48173/99 and 48319/99 at §47.

i) Legitimate aim

In the context of criminal proceedings, the publication of personal data might be deemed to serve the legitimate aim of investigating and prosecuting crime. For example, a photograph and personal information about an accused person might be published to assist with the gathering of further information relevant to an ongoing investigation, to identify if further offences have been committed, or as part of efforts to locate a suspect. Further, the publication of such information might be deemed to help prevent the commission of further offences and to protect the rights and freedoms of others, by dissuading the public from approaching or engaging with the suspect.[148]

However, it is necessary to ensure that, where a photograph is published in the context of reporting on criminal proceedings, it does serve some informational or investigative value. For example, where the accused is already detained in custody, the showing of their photograph cannot be justified by reference to the aim of protecting the public from that person or enlisting public support to determine their whereabouts.[149] This situation can be contrasted with the situation of a suspect who has been released on bail, or whose whereabouts is unknown, for example.[150]

Additionally, the publication of personal information might be deemed to serve the aim of reducing or deterring non-compliance with civil rules and regulations. For example, publishing the names, addresses and financial data of major tax debtors to deter non-compliance with tax regulations and encourage people to pay their taxes.[151]

ii) Proportionality

When assessing whether the publication of information is necessary in a democratic society and whether or not it is a proportionate means of achieving the legitimate aims described above, it is necessary to take account of the following factors:[152]

[148] *Margari v. Greece*, judgment of 20 June 2023, no. 36705/16 at §§47-49 and 52 (included as a summary in this publication).

[149] *Khuzhin and Others v. Russia*, judgment of 23 October 2008, no. 13470/02 at §117.

[150] *Margari v. Greece*, judgment of 20 June 2023, no. 36705/16 (included as a summary in this publication).

[151] *L.B. v. Hungary*, Grand Chamber judgment of 9 March 2023, no. 36345/16 at §§108-114 (included as a summary in this publication).

[152] *L.B. v. Hungary*, Grand Chamber judgment of 9 March 2023, no. 36345/16 at §§118 – 122 (included as a summary in this publication).

- The extent to which publication of the information represents a measure targeted at an individual, or forms part of a general scheme. The adoption of general measures within a wider legislative scheme concerning publication of information relating to people who fall into pre-defined situations is more likely to be proportionate than measures targeting certain individuals.
- Whether or not the publication of information is subject to a time limit.
- The extent to which a particularly important facet of an individual's identity is at stake, for example:
  - Intimate information, such as health data, sexual orientation and religious attitudes should merit from heightened protection.
  - A person's financial data is not deemed to constitute intimate details about their life and does not merit enhanced protection.
- The repercussions of the publication of the information on a person's private life, for example, the extent to which they experience feelings of insecurity, humiliation and exclusion from public life as a result of its publication.
- The level of public interest in the dissemination of the information and the seriousness of the issue at stake, for example, the seriousness of the criminal offence or breach of civil regulations that the publication of information seeks to deter.
- The medium used to disseminate information, for example printing information in the printed press will normally be deemed to have less of an impact than publishing information on the internet.
- The breadth of the audience that accesses the medium used to publish the information.
- The existence of procedural safeguards, for example notification to an individual that their information or photographed will be published, offering the chance to object or the right of an appeal to assert that their Article 8 rights have been breached.

The following principles of data protection law are also relevant to any assessment of proportionality:[153]

- **Purpose limitation:** any processing of personal data must be done for a specific, well-defined purpose, and only for additional purposes which are compatible with the original purpose.

[153] *L.B. v. Hungary*, Grand Chamber judgment of 9 March 2023, no. 36345/16 at §§123 (included as a summary in this publication).

- **Data minimisation:** personal data published should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- **Data accuracy:** recognising that inaccurate or false information contained in public registers can be injurious or potentially damaging to the data subject's reputation, statutory procedural safeguards for the correction and revision of the information must be in place.
- **Storage limitation:** personal data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed. The initial lawful processing of accurate data may over time become incompatible with the requirements of Article 8 where those data are no longer necessary for the purposes for which they were collected or published.

Application of the above principles in the context of criminal proceedings

The publishing and processing of personal data relating to criminal charges calls for enhanced protection because of the particular sensitivity of the data at issue. When sensitive data is being published in the context of pending criminal proceedings or in the context of the investigation of criminal offences, it is therefore imperative that the data published accurately reflects the situation and the charges pending against an accused person, regard also being had to the observance of the presumption of innocence.

c) The right to a public hearing under Article 6(1)

Article 6 ECHR guarantees the right to a "*fair and public hearing*".

The right to a "public hearing" and the principle of publicity under Article 6 entail two aspects: the holding of public hearings (discussed below) and the public delivery of judgments (discussed in the following section of this publication).[154]

The public character of proceedings is a fundamental principle in any democratic society. It is essential to enable public scrutiny of the administration of justice and to maintain confidence in the courts.[155] Normally, to comply with the requirement of publicity, the public must be able to obtain information about

[154] *Sutter v. Switzerland*, judgment of 22 February 1984, no. 8209/78 at §27.

[155] *Riepan v. Austria*, judgment of 14 November 2000, no. 35115/97 at §27.

the date, time and place of hearing, and the hearing must be easily accessible to the public.[156] The public nature of judicial proceedings can, however, give rise to concerns regarding the protection of the confidentiality of a person's personal data, which might be discussed or disclosed at a public hearing. National authorities must strike a fair balance between, on the one hand, protecting the public nature of proceedings in accordance with Article 6, and on the other hand, protecting the interests of a party to proceedings, or of a third party, in maintaining the confidentiality of his or her data in accordance with Article 8.[157] This might involve: i) implementing limits on the type and scope of data disclosed at a hearing; or ii) in certain circumstances, States might deem it necessary to hold a hearing in camera.

i) Limiting the information disclosed at a hearing

The admission of personal and sensitive data as evidence in a public hearing can constitute an interference with Article 8 ECHR, as this involves disclosing such information to the public.

In order to comply with Article 8 in this context, the disclosure of personal data must be in accordance with law, serve a legitimate aim, and must be limited so far as possible to what is rendered strictly necessary by the specific features of the proceedings and by the facts of the case.[158]

Legitimate Aim

The disclosure of personal data during public proceedings, even including sensitive medical data, might be necessary to pursue the legitimate aim of protecting the rights and freedoms of others. In particular, the right to produce evidence in order to pursue a claim before the courts.[159] The pursuit of this aim requires the disclosure of enough information to provide a judge with sufficient knowledge of a case to rule on its merits and to ensure the smooth running of judicial proceedings.[160]

[156] *Riepan v. Austria*, judgment of 14 November 2000, no. 35115/97 at §29.

[157] *C.C. v. Spain*, judgment of 6 October 2009, no. 1425/06 at §35.

[158] *L.L. v. France*, judgment of 10 October 2006, no. 7508/02 at §45 (included as a summary in this publication).

[159] *L.L. v. France*, judgment of 10 October 2006, no. 7508/02 at §40 (included as a summary in this publication).

[160] *C.C. v. Spain*, judgment of 6 October 2009, no. 1425/06 at §29.

Proportionality

In determining the extent to which disclosure of personal data is rendered "strictly necessary" by the facts and features of a case, it is necessary to take account of the type of personal data in question, the nature of proceedings, and the extent to which the data is decisive to the determination of case. For example, the protection of sensitive or special categories of data, such as sensitive health data, is deemed to be of vital importance, and such data should benefit from heightened protection.[161] On the other hand, certain types of proceedings, for example family and divorce proceedings, necessarily require courts to engage with individuals' most intimate private information, and so to interfere with their private and family life, in order to determine the types of disputes before them.[162]

Where disclosure of sensitive data is deemed to be required, this must be limited to what is rendered strictly necessary to resolve the case. The key test is: i) whether the judge would have sufficient knowledge to resolve the case even without disclosure of the sensitive evidence; and ii) whether the judge would have reached the same conclusion with or without disclosure of the sensitive data.[163]

ii) In camera hearings

The requirement to hold a public hearing is subject to some permitted exceptions. In certain circumstances, it might be necessary to exclude the public and the press from a hearing to protect the right to private life of the parties

[161] *L.L. v. France*, judgment of 10 October 2006, no. 7508/02 at §44 (included as a summary in this publication).

[162] *L.L. v. France*, judgment of 10 October 2006, no. 7508/02 at §45 (included as a summary in this publication).

[163] *Contrast L.L. v. France*, judgment of 10 October 2006, no. 7508/02 (included as a summary in this publication) with *C.C. v. Spain*, judgment of 6 October 2009, no. 1425/06. In the former case, disclosure of sensitive medical data breached Article 8 because such data was not deemed to be necessary to resolve the case. The domestic courts' decision to grant a divorce was based on a range of evidence, most notably witness testimonies, and it was therefore found that, even if the contested evidence was declared inadmissible, the courts would have reached the same conclusion. In the latter case, the disclosure of the applicant's medical data did not breach Article 8. The case concerned a compensation payment on account of the applicant's incapacity to work (and so his medical condition / history). His medical file therefore contained the information which formed the subject-matter of proceedings, and its disclosure was necessary to examine and decide the case.

involved. It might also be necessary to limit attendance rights to safeguard the overall fairness of proceedings under Article 6. For example, where publicity inhibits the ability of parties to participate effectively in the hearing.[164]

Article 6 (1) provides:

> *"The press and public may be excluded from all or part of the trial … where the interests of juveniles or 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."*

Even in the context of criminal proceedings, where there is a heightened emphasis on the need for publicity, it is possible to limit the open and public nature of proceedings, for example, to protect the safety or privacy of witnesses or to promote the free exchange of information and opinion in the pursuit of justice.[165]

It is necessary to show, however, that the decision to hold a hearing either wholly or partly in camera is strictly required, taking account of all the circumstances of the case.[166] Relevant circumstances include the age and vulnerability of those involved. It is also relevant to take account of the extent to which the parties will be required to express themselves candidly on highly personal issues without fear of public curiosity or comment, in order for the judge to make a fully informed decision with an accurate grasp of all the relevant facts.[167] In this context, it could even be permissible for States to operate a general presumption in favour of in camera hearings for certain classes of cases, for example where children are

[164] *T. v. the United Kingdom*, judgment of 16 December 1999, no. 24724/94, where the criminal trial of a child attracted high levels of media and public interest and the applicant was found to be unable to participate effectively in the criminal proceedings against him, in breach of his right to a fair hearing in breach of Article 6 § 1. It was found that the hearing should have been conducted in such a way as to reduce as far as possible his or her feelings of intimidation and inhibition, for example by providing for selected attendance rights.

[165] *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 at §37 (included as a summary in this publication).

[166] *Kilin v. Russia*, judgment of 11 May 2021, no. 10271/12, §§111-112; *Martinie v. France*, Grand Chamber judgment of 12 April 2006, no. 58675/00 at §40.

[167] *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 at §38 (included as a summary in this publication).

involved, in order to protect the interests of juveniles, the private life of parties and the overall fairness of proceedings.[168]

It is, however, essential that there are procedural protections in place which mean that it is possible to apply for judicial review of any decision to hold a hearing in camera, and that there is always at least the possibility of holding a hearing in public where it is deemed necessary following such review.[169]

Conversely, a decision to hold a hearing in public, rather than in camera, might breach a person's Article 8 rights, where the public hearing involves examining their personal and sensitive information. Procedural protections are equally important in this context. Where a person requests that a hearing take place in camera, courts should undertake an individualised proportionality assessment to determine if a public hearing, and the resultant interference with a person's Article 8 rights, is necessary, taking account of all the circumstances of the case. This individualised proportionality assessment should seek to balance the importance of transparent proceedings with the importance of respecting the confidentiality of personal information. Courts should take account of the extent to which the disclosure of sensitive information is required to determine the case (as discussed in the section above). Limiting the scope of personal data disclosed during proceedings might be one way to retain their public nature, whilst also limiting the impact on a person's Article 8 rights. Where disclosure cannot be limited (as discussed in the section above)[170] an in camera hearing might be considered necessary. What is important from the perspective of Article 8 is to have in place a procedure to properly consider these questions following a request for an in camera hearing, which results in a properly reasoned and justified response to such a request.[171]

[168] *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 at §39 (included as a summary in this publication); *Campbell and Fell v. the United Kingdom*, judgment of 28 June 1984, nos. 7819/77 and 7878/77 at §§87-88.

[169] *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 at §39 (included as a summary in this publication).

[170] *C.C. v. Spain*, judgment of 6 October 2009, no. 1425/06.

[171] *Frâncu v. Romania*, judgment of 13 October 2020, no. 69356/13 at §§62-75.

The right to review of the lawfulness of detention under Article 5

Issues regarding the publication of confidential or sensitive data can also emerge in the context of proceedings arising from the right to have the lawfulness of detention speedily examined by a court under Article 5(4) ECHR.

The case of *A and others v. the United Kingdom*[172] highlights how two of the issues discussed earlier in this publication in the context of Article 6 (limiting the disclosure of sensitive material during proceedings and holding hearings in camera) might also arise in respect of the rights protected under Article 5. The 11 applicants were detained under an extended power created by the UK government permitting their detention where the Secretary of State reasonably believed that their presence in the UK was a risk to national security and reasonably suspected that they were an international terrorist.[173]

The decision to detain an individual was subject to review every 6 months before the Special Immigration Appeals Commission ("**SIAC**"). The SIAC was able to consider evidence which could be made public (the open material) and sensitive evidence which could not be disclosed for reasons of national security (the closed material). The detainee and his legal team had access to the open material and could comment on it in writing and at a hearing. The closed material was only disclosed to a special advocate, appointed on behalf of each detainee by the Solicitor General. The SIAC held both open and closed hearings. In the closed hearings, the SIAC would consider the closed material and the special advocate could make procedural and substantive submissions on behalf of the detainee. Once the special advocate had access to the closed material, he was not permitted any contact with the detainee or his lawyers without leave of the court.

The SIAC dismissed the applicants' appeals against their detention. The applicants argued that the SIAC procedure was incompatible with Article 5(4) ECHR on the basis that the procedure was unfair because they did not have full disclosure of the evidence against them.

The ECtHR accepted that at the relevant time there was an urgent need to protect the UK population from terrorist attacks and a strong public interest in obtaining

[172] *A and others v. the United Kingdom*, Grand Chamber judgment of 19 February 2009, application no. 3455/05.

[173] The UK Government issued a derogation notice under Article 15 in respect of Article 5(1) ECHR.

information about al-Qaeda whilst maintaining the secrecy of the sources. This had to be balanced against the applicants' rights under Article 5(4) ECHR.

The ECtHR held that it was essential that as much information about the allegations and evidence against each applicant was disclosed as possible without compromising national security or the safety of others. Where full disclosure was not possible, each applicant must still be given the possibility to effectively challenge the allegations against him. The SIAC, a fully independent court, was best placed to ensure that no material was unnecessarily withheld from the detainee; whilst the special advocate provided an important, additional safeguard to counterbalance the lack of full disclosure and lack of a full, open, adversarial hearing. The ECtHR accepted that the secrecy employed and the lack of disclosure in respect of each applicant was justified and proportionate.

However, the ECtHR found that the special advocate could not undertake his function properly where the open material consisted of purely general assertions and the SIAC's decision was based on closed material. For example, in respect of certain applicants, the open material contained sufficiently detailed allegations about, for example, the purchase of specific telecommunications equipment, to enable the applicants to effectively challenge them. By contrast, in respect of other applicants who faced allegations that they had been involved in fundraising for terrorist groups, the evidence which provided the link between the money raised and terrorism was not disclosed and therefore, they could not effectively challenge the allegations.

An essential safeguard in this context is, therefore, that an applicant must be provided with sufficient information about the allegations against him to enable him to give effective instructions to his legal representative.

d) The right to public pronouncement of judgments under Article 6(1)

Article 6 ECHR provides that "*Judgment shall be pronounced publicly*".

The right to public procurement of a judgment is a freestanding right under Article 6, which is separate from the right to a public hearing (discussed above). So, if a hearing is unjustifiably held in camera, public pronouncement of the judgment cannot be used to remedy the breach of a right to a public hearing.[174]

[174] *Artemov v. Russia*, judgment of 3 April 2014, no. 14945/03 at §109.

i) What constitutes public pronouncement of judgment?

The words "pronounced publicly" do not need to be interpreted literally, meaning that judgments do not need to be read aloud in open court. There is some flexibility regarding how judgments can be pronounced. However, the complete concealment from the public of the entirety of a judicial decision is unlikely to ever be justified.[175]

The form of publicity required under Article 6(1) depends on the circumstances of a case and the specific features of proceedings. It must be assessed in light of the overall aim of the provision, which is to ensure scrutiny of the judiciary by the public to help safeguard the right to a fair trial and guard against arbitrariness.[176] Courts must also take account of the requirements of Article 8 ECHR when interpreting and implementing the right to publicity under Article 6 (discussed below).

Generally, as a minimum, the public should be able to access copies of at least the operative parts of a judgment. The concept of public pronouncement can, therefore, include depositing the text of a judgment in a court registry or website which can be accessed by anyone.[177] In a criminal context, it can include reading out a criminal sentence at a public hearing and later filing the reasons for the decision at the court registry, where the sentence read out contained sufficient information on the charge, finding of guilt, the presence of aggravating circumstances and the penalty imposed.[178]

The nature of the proceedings as a whole is relevant to determining whether the requirement of public procurement has been complied with. This includes the age and vulnerability of the parties involved, whether or not a public authority is party to the case, and the extent to which any of the stages of proceedings have taken place in public.

For example, in cases between individual parties concerning the residence of children, and where it has already been found to be justified for a hearing to

[175] *Raza v. Bulgaria*, judgment of 11 February 2010, no. 31465/08 at §53.

[176] *Pretto and Others v. Italy*, judgment of 8 December 1983, no. 7984/77 at §§21 and 26; *Raza v. Bulgaria*, judgment of 11 February 2010, no. 31465/08 at §53.

[177] *Pretto and Others v. Italy*, judgment of 8 December 1983, no. 7984/77 at §§27-28.

[178] *Crociani and Others v. Italy* (dec.), decision of 18 December 1980, nos. 8603/79, 8722/79, 8723/79 and 8729/79.

take place in camera, access to court orders and judgments containing private information about the residence of children can be limited to only those who can establish an interest.[179] In such circumstances, courts should at least make judgments of special interest accessible to the wider public.[180] By contrast, where a state authority is a party to proceedings, there is a greater need for a judgment to be accessible by all of the public and limiting access to those with a legal interest in the case is less likely to be compliant with Article 6.[181] It is particularly important in the context of proceedings against state authorities for the public (as well as the parties) to have access to the reasoning behind a judgment, in addition to its operative parts.[182]

National Security Cases

In the context of national security cases, it may sometimes be necessary to classify parts of a judgment referring to confidential material. However, the complete concealment from the public of the entirety of a judicial decision in such proceedings cannot be regarded as warranted. States must only classify / redact the parts of their decisions whose disclosure would compromise national security or the safety of others. They must adopt techniques to accommodate legitimate security concerns without fully negating fundamental procedural guarantees such as the publicity of judicial decisions.[183]

---

[179] *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 at §47 (included as a summary in this publication). See also *Sutter v. Switzerland*, judgment of 22 February 1984, no. 8209/78, where, taking account of the particular nature of military proceedings, the Court found that the publicity requirement was satisfied by the fact that anyone who established an interest could consult or obtain a copy of the full text of the Military Court of Cassation. It was also relevant that a public hearing had been held by the lower instance court.

[180] *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 at §47; *Sutter v. Switzerland*, judgment of 22 February 1984, no. 8209/78 at §34 (included as a summary in this publication).

[181] *Moser v. Austria*, judgment of 21 September 2006, no. 12643/02 at §§101-103, the case concerned the transfer of custody of a child to the state, by contrast to the case of *B. and P. v. the United Kingdom*, judgment of 24 April 2001, nos. 36337/97 and 35974/97 (included as a summary in this publication) which was a dispute between individuals.

[182] *Ryakib Biryukov v. Russia*, judgment of 17 January 2008, no. 14810/02.

[183] *Raza v. Bulgaria*, judgment of 11 February 2010, no. 31465/08 at §53; *Vasil Vasilev v. Bulgaria*, judgment of 16 November 2021, no. 7610/15; *Fazliyski v. Bulgaria*, judgment of 16 April 2013, no. 40908/05.

Hearings involving Covert Surveillance and Intercept Evidence

States can also limit the extent to which a judgment is made public in the context of criminal trials involving evidence obtained from covert police operations. It is recognised that States have a legitimate interest in prosecuting offences and that they may need to take measures to keep secret the police's methods of surveillance and investigation. In this context, where publication of the reasoning behind a decision would prejudice the effective operation of secret police investigation and surveillance methods, courts are permitted to restrict access to the full judgment (including their reasoning) to the parties alone. Courts must still, however, make the operative parts of their judgment available to the public, including for example, information about the applicants, the charges against them and their legal classification, the findings as to their guilt and sentence and the order for costs.[184]

ii) Delivering judgments: striking the balance between a fair trial and data protection

The public pronouncement of a judgment has the potential to infringe upon the rights to protection of personal data, physical and moral integrity, reputation and honour of those who are referenced in a judgment. The public pronouncement of a judgment must not interfere with these rights beyond the extent to which it is necessary to pursue a legitimate aim.

When is Article 8 engaged?

In this context, the protections under Article 8 extend not only to the parties to the proceedings, but also to any other third party whose identity or personal information is referenced in a judgment.[185]

Article 8 is engaged where a person is identified by name in a judgment alongside information which falls within the scope of personal data (as described earlier in this publication) or statements which damage their reputation or honour.[186] It is

[184] *Welke and Białek v. Poland*, judgment of 1 March 2011, no. 15924/05 at §§83-84.

[185] *Z. v. Finland*, judgment of 25 February 1997, no. 22009/93; *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 (included as a summary in this publication).

[186] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 (included as a summary in this publication), where the applicant was named in a judgment and described as having committed conduct which

also engaged where a person is not identified by name, but they are identifiable as a result of other information published in a judgment. For example, where an individual whose personal data is discussed in a judgment is referred to as the spouse or other family member of a person who is named in the judgment, and so becomes identifiable by association.[187]

Article 8 cannot, however, be relied upon to complain of a loss of reputation which is the foreseeable consequence of one's own actions. For example, an individual cannot generally complain under Article 8 that their reputation has been prejudiced by publication of a judgment in which they are convicted of a criminal offence, or which finds them to have carried out conduct they have been accused of during civil proceedings.[188]

Legitimate Aim

The publication of personal information relevant to a judgment can serve the legitimate aim of ensuring the transparency of court proceedings and thereby maintaining the public's confidence in the courts.[189] Publishing information about a person's conduct might also serve the aim of "the protection of the rights and freedoms of others" by acknowledging and publicly disclosing the facts as a way of reparation for the damage suffered by the victim of that conduct and in the interests of the proper administration of justice.[190]

Proportionality

To assess whether an interference with Article 8 is proportionate in this context, it is necessary to examine if there are sufficient cogent reasons to justify the disclosure of personal information. This involves examining if the court had the ability to adopt any protective measures which would have limited the impact on a person's rights to private and family life whilst maintaining respect for the principle of publicity under Article 6 (1).

---

amounted to psychological harassment and bullying.

[187] *Z. v. Finland*, judgment of 25 February 1997, no. 22009/93, where the applicant was not named in the judgment, but her husband's full name was included which meant that the reference to his "wife" "as an HIV carrier" breached her Article 8 rights to private and family life.

[188] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §41 (included as a summary in this publication).

[189] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §45 (included as a summary in this publication).

[190] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §45 (included as a summary in this publication).

For example, courts can anonymise judgments, by omitting any names permitting identification of an individual and replacing them with initials. They can also publish an abridged version of a judgment, containing the operative parts of the decision and any relevant legal analysis, whilst limiting access to the full reasoning of the judgment.[191]

States will be in breach of Article 8 where courts have the option to take such measures, but choose not to do so, without any cogent reason as to why.[192] The following factors will also be relevant to an assessment of proportionality in this context.

- Whether the personal information was relevant / determinative to the conclusions in the judgment.[193]
- The impact of disclosure on the person concerned, including the impact on their personal and professional situation, honour and reputation and the extent to which it would lead them to be stigmatised or ostracised by their community.[194]
- The scope of the media coverage and public interest in the case and the likely size of the audience who will read the judgment.[195]
- Where the judgment refers to a third party, whether effective procedural safeguards are in place, such as notification procedures to inform the person of the proceedings and the existence of a mechanism enabling a person to request the non-disclosure of their identity or personal information prior to the publication of judgment.[196]

---

[191] *Z. v. Finland*, judgment of 25 February 1997, no. 22009/93; *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 (included as a summary in this publication).

[192] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 (included as a summary in this publication); *C.C. v. Spain*, judgment of 6 October 2009, no. 1425/06.

[193] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §§47 and 49 (included as a summary in this publication).

[194] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §48 (included as a summary in this publication).

[195] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §§48 and 54 (included as a summary in this publication).

[196] *Vicent Del Campo v. Spain*, judgment of 6 November 2018, no. 25527/13 at §53 (included as a summary in this publication).

iii) Anonymisation of judgments

This section provides a comparative overview of the procedures implemented by certain courts (at both the European and domestic level) to govern anonymisation of their judgments and to help ensure that publication of judgments does not interfere to an unnecessary extent with Article 8 rights.

The European Court of Human Rights

All information in proceedings before the ECtHR is public unless anonymity has been authorised by that court. A request for anonymity may be made by an applicant in respect of their identity and documents in the proceedings on the application form or as soon as possible thereafter. However, the ECtHR can also act of its own motion. If an applicant makes an anonymity request, they must provide reasons in writing justifying the derogation from the normal rule of public access and specify the impact that publication of the ECtHR's judgment may have on them.

The ECtHR's procedural rules also allow for retroactive anonymity requests. If an applicant wishes to make such a request, they must explain the reasons for the request and specify the impact of publication, and also set out why anonymity was not requested while the case was pending before the ECtHR. The President will consider the applicant's explanations, the level of publicity the case has already received and whether it is appropriate or practical to grant the request. If the President authorises the request, they will also determine the steps to be taken to protect the applicant from being identified.

In order to protect private life, the President is also permitted to "take any other measure [they] consider necessary or desirable" with respect to the ECtHR's publications.[197]

[197] Rule 47 of the Rules of the Court dated 23 June 2023, available at https://t.ly/HKYxc. §12(a) of the Institution of Proceedings practice direction issued by the President of the Court in accordance with Rule 32 of the Rules of Court on 1 November 2003 and amended on 22 September 2008, 24 June 2009, 6 November 2013, 5 October 2015, 27 November 2019, 25 January 2021 and 1 February 2022. This practice direction supplements Rules 45 and 47, available at https://t.ly/HKYxc, pp.60-62.Requests for anonymity practice direction issued by the President of the Court in accordance with Rule 32 of the Rules of Court on 14 January 2010, available at https://t.ly/HKYxc, p.73.

The Court of Justice of the European Union

Where anonymity has been granted by the referring court, the CJEU will respect the anonymity. The CJEU may also grant anonymity in respect of personal data at the request of the referring court, as part of the main proceedings or of its own motion. The anonymity can be in relation to one or more persons or entities concerned by the case.[198]

In the Practice Directions[199] to the parties, the CJEU notes that as a general rule it deals with cases in anonymised form in order to protect personal data. If a party to the proceedings wishes to anonymise their identity or certain details concerning them, that party may apply to the CJEU. The CJEU will then decide whether to anonymise the relevant case, in whole or in part, or maintain the anonymity as is.

The application for anonymity must be made as soon as possible in the proceedings because anonymity becomes more difficult once notice of the case or the request for a preliminary ruling has been served on interested persons, about a month after the request has been lodged at the CJEU.

The United Kingdom

The UK judiciary processes data consistently with data protection law; however, subject access rights under the UK General Data Protection Regulation do not apply to personal data processed by the judiciary in exercising judicial functions.[200]

The general rule is that court proceedings take place in public, to which the public and the media have the right to attend, and the media is able to report the proceedings fully and contemporaneously. Any restrictions to this general rule are exceptional: it must be necessary and proportionate.[201] Where this test is

[198] Article 95 of the Rules of Procedure of the Court of Justice of 25 September 2012, as amended on 18 June 2013, on 19 July 2016, on 9 April 2019 and on 26 November 2019, available at: https://t.ly/lWB7g.

[199] §§7-9 of the Practice Directions to Parties concerning Cases brought before the Court of 14 February 2020, available at https://t.ly/lWB7g.

[200] Lord Chief Justice of England and Wales and the Senior President of Tribunals, "Judiciary and Data Protection: privacy notice", available at: https://t.ly/qhG_j.

[201] Judicial College, "Reporting Restrictions in the Criminal Courts" (September 2022), p.9, available at: https://

met, the court may restrict personal data in its judgment, hold legal proceedings in private, or place restrictions on access to court files. Any decisions regarding restrictions can only be taken during legal proceedings.[202]

In criminal proceedings, the court may, of its own initiative or at the request of a party, restrict reporting of or public access to a hearing or withhold information in an otherwise public hearing. The party must make such a request in writing as soon as possible, setting out the power the court has to derogate from the general rule and explaining why it is necessary. For example, in respect of restricting reporting of certain information in criminal proceedings for the lifetime of witnesses and victims under the age of 18, the party must explain why such restrictions would improve the quality of the evidence given or the level of cooperation by the witness/victim. The factors to be considered are, amongst other things, the nature and alleged circumstances of the offence, the witness or victim's age, their social and cultural background and ethnic origins. The information which may not be reported include the name, address, educational establishment attended and place of work of the witness/victim.[203]

In exceptional circumstances, criminal proceedings may be held in private. The party requesting this must apply not less than five business days before the trial, explaining why private proceedings are necessary and why no other measures would suffice. The test is whether proceeding in private is necessary to avoid the administration of justice from being frustrated or rendered impractical. It is insufficient that proceeding in public will cause embarrassment to or damage individuals' reputations. The test cannot be met if the consequence of holding proceedings in private would be an unfair trial. The media is given an opportunity to make representations.[204]

tinyurl.com/3endbhpk.

[202] Lord Chief Justice of England and Wales and the Senior President of Tribunals, "Judiciary and Data Protection: privacy notice", available at: https://t.ly/qhG_j.

[203] Section 45A Youth Justice and Criminal Evidence Act 1999; rule 6.4 Criminal Procedure Rules 2020.

[204] Rules 6.6-6.7 Criminal Procedure Rules 2020; Judicial College, "Reporting Restrictions in the Criminal Courts", 2022, pp.11-12, available at: https://tinyurl.com/3endbhpk.

Germany

The German Federal Constitutional Court may provide information from or access to its files to:

» public entities, to the extent necessary for the administration of justice (amongst other reasons); and
» individuals and other non-public entities once proceedings are finished, provided they can prove a legitimate interest and the data protection interests of third parties are safeguarded.

Access to files is only granted where providing information from the files is insufficient for the requesting public entity to fulfil its tasks or where it would not satisfy the legitimate interests of the individual or other non-public entity, or where providing the information would require a disproportionate effort.

Where the information requested is not part of the case file, the requesting party must demonstrate that the entity whose files are at issue consented to that information being transferred to that party.

Personal data held by the Federal Constitutional Court within its files is protected by the general data protection law. Subjects therefore have a right to access their personal data and a right to rectify inaccurate data. However, the erasure of personal data may only be requested where the personal data is no longer needed (i.e. court proceedings are finished and statutory retention periods do not apply or have been met), it is processed unlawfully or the relevant consent has been withdrawn.

iv) Anonymisation of judgements and Article 10 ECHR

The key case in this area is the recent judgment of the Grand Chamber in *Hurbain v. Belgium*,[205] which is addressed in the section below.

[205] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 (included as a summary in this publication).

Chapter 5

The right to be forgotten and the right to erasure

The right to be forgotten

The evolving content, and the importance to the individual, of the "right to be forgotten" - or a right to erasure of data - has been set out most recently by the Grand Chamber in *Hurbain v. Belgium*. The Grand Chamber stated that:

> "For a number of years now, with the development of technology and communication tools, a growing number of persons have sought to protect their interests under what is known as the "right to be forgotten". This is based on the individual's interest in obtaining the erasure or alteration of, or the limitation of access to, past information that affects the way in which he or she is currently perceived. By seeking to have that information disappear, the persons concerned wish to avoid being confronted indefinitely with their past actions or public statements, in a variety of contexts such as, for instance, job-seeking and business relations."[206]

The Grand Chamber recognised that personal information that is published and has been available on the Internet for some time may have a far-reaching negative impact on how the person concerned is perceived by public opinion.[207] There are also other risks, such as the risk of the aggregation of information which may lead to the creation of a profile of the person concerned and further, that those reading an online article, out of context, can receive a fragmented and distorted picture

[206] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §191 (included as a summary in this publication).

[207] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §192 (included as a summary in this publication).

of reality. There is also the constant threat and the resulting fear for the individual concerned of being unexpectedly confronted with his or her past at any time.

The Grand Chamber noted that the concept of a right to be forgotten has many facets and is still under construction.[208] The Grand Chamber also set out that the right may give rise in practice to various measures that can be taken by search engine operators or by news publishers.[209] These can relate either to the content of an archived article (for instance, the removal, alteration or anonymisation of the article) or to limitations on the accessibility of the information. In the latter case, limitations on access may be put in place by both search engines and news publishers. The Grand Chamber clarified that it would use the term "delisting" to refer to measures taken by search engine operators, and "de-indexing" to denote measures put in place by the news publisher responsible for the website on which the article in question is archived.

The focus of this section is on investigative and judicial proceedings. Cases in this area have arisen in two broad contexts. First, cases stemming from the operation of the State's criminal and civil justice system and associated record-keeping. Second, cases concerning journalists and newspapers, stemming from content published about individuals who have been the subject of criminal or civil investigation or proceedings. The key cases can be broken down further into the following categories:

1) Individuals who had been under investigation by police, or had been suspected or accused of committing criminal or civil offence.
2) Individuals who had been convicted of an offence.
3) Individuals in respect of whom security services have collated and retained information.
4) Individuals who had been the subject of journalistic coverage as a result of investigation, arrest, or conviction.

[208] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §194 (included as a summary in this publication).

[209] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §175 (included as a summary in this publication).

The sources of the right to be forgotten

In Convention cases, individuals who have sought to erase information about themselves in the public domain have relied upon Article 8, the right to respect for private and family life. As to this, the Grand Chamber stated in *Hurbain* that a claim of entitlement to be forgotten does not amount to a self-standing right protected by the Convention and, to the extent that it is covered by Article 8, can concern only certain situations and items of information.[210]

The Grand Chamber set out key international instruments on the right to be forgotten at paragraphs 17-80 of its judgment. This includes some of the key data protection instruments discussed in part 2 of this publication, such as Convention 108, Convention 108+ and the GDPR.

It also includes instruments more specifically related to the right to be forgotten, such as:

United Nations instrument

» The Universal Declaration on Archives was initiated by the International Council on Archives and adopted by UNESCO ON 10 November 2011. This non-binding declaration provides a definition of archives that includes all recorded decisions, actions and official documents in all formats including paper, digital and audiovisual. The aims it identifies include ensuring that archives are (i) managed and preserved in ways that ensure their authenticity, integrity and usability, and (ii) made accessible to everyone, while respecting the pertinent laws and the rights of individuals.

Council of Europe instruments

» Recommendation No. R (2000) 13 of the Committee of Ministers, which recommends that States enact legislation on access to archives which balances the conflicting requirements of transparency and secrecy, the protection of privacy and access to historical information.
» Recommendation Rec(2003)13 of the Committee of Ministers on the provision of information through the media in relation to

[210] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §199 (included as a summary in this publication).

criminal proceedings, which stresses the importance of media reporting in informing the public on criminal proceedings, making the deterrent function of criminal law visible and ensuring public scrutiny of the functioning of the criminal justice system.

» Recommendation Rec (2012) of the Committee of Ministers on the protection of human rights with regard to search engines, which, whilst stressing the importance of search engines for rendering content on the Internet useful and accessible, also notes the impact of search engines on the right to private life and the protection of personal data, stemming from the pervasiveness of search engines and from data retention.

European Union law instruments and guidelines

» The European Data Protection Board's Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR, 7 July 2020.
» Guidelines on the implementation of the CJEU judgment in the case of *Google Spain SL and Google Inc v. Agencia Espanola de Proteccion de Datos and Gonzalez*,[211] adopted on 26 November 2014.

The significance of freedom of expression to the right to be forgotten

Journalists and newspapers have sought to rely on freedom of expression under Article 10 to resist individuals' requests for erasure or, as in *Hurbain*, anonymisation of articles. In these cases, the Court has recognised the tensions between Article 8 and Article 10, and has considered whether domestic courts identified and engaged sufficiently with relevant considerations when reaching their decision.

The Grand Chamber in *Hurbain* stressed the importance of freedom of expression.[212] It reiterated that freedom of expression constitutes one of the essential foundations of a democratic society and one of the basis conditions for its progress and for each individuals' self-fulfilment. It stated that as regards press

[211] (C-131/12) *Google Spain SL and Google Inc v. Agencia Espanola de Proteccion de Datos and Gonzalez*, Grand Chamber judgment of 13 May 2014.

[212] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §§176-179 (included as a summary in this publication).

freedom, although the press must not overstep certain bounds, particularly as regards the reputation and rights of others, its duty is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest. Thus, the task of imparting information necessarily includes duties and responsibilities as well as limits which the press must impose on itself spontaneously. The public also has a right to receive this information and these ideas. The press must be able to play the vital role of "public watchdog" and particularly strong reasons must be provided for any measure limiting access to information which the public has the right to receive. The Grand Chamber stressed that it was not for the Court, any more than it is for the national courts, to substitute its own views for those of the press as to what techniques of reporting should be adopted in a particular case or how the profession should be exercised, including means of transmission of opinions or information.

The Grand Chamber highlighted in detail the importance of the preservation of archives. It emphasised that in addition to the press's primary function as a "public watchdog", the press has a secondary, also valuable role in maintaining archives containing news which has previously been reported and making them available to the public.[213] 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. This function of the press, like the corresponding legitimate interest of the public in accessing the archive, is protected by Article 10.

Even in the context of a defamatory publication the Grand Chamber noted that the Court has held that it is not in the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.

The Grand Chamber noted the emergence over the past decade of a consensus regarding the importance of press archives. In the context of the processing of personal data at European Union level, the GDPR makes express provision for an exception to the right to the erasure of personal data where the processing of

[213] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §§180 and 182-186 (included as a summary in this publication).

the data is necessary for the exercise of the right of freedom of expression and information. It requires EU member States to provide exemptions or derogations in their legislation for processing carried out for journalistic purposes if they are necessary to reconcile the right to the protection of personal data with freedom of expression and information. In the same vein, in the Council of Europe context, the explanatory report to Convention 108+ specifies that the exceptions and restrictions provided for in Article 11 of that Convention should apply in particular to the processing of personal data in news archives and press libraries.

The Grand Chamber stressed that since the role of archives is to ensure the continued availability of information that was published lawfully at a certain point in time, they must, as a general rule, remain authentic, reliable and complete. The integrity of digital press archives should be the guiding principle underlying the examination of any request for the removal or alteration of all or part of an archived article which contributes to the preservation of memory, especially if (as was the case in *Hurbain*) the lawfulness of the article has never been called into question. National authorities must be particularly vigilant in examining requests, grounded on respect for private life, for removal or alteration of the electronic version of an archived article whose lawfulness was not called into question at the time of its initial publication. Such requests call for thorough examination.

The Court's analysis when determining whether there has been a violation of the right to be forgotten

In each case before it, the Court applies its usual analysis in order to determine whether there has been a violation of a Convention right. The stages of analysis are as follows:

1) Whether there has been an interference.
2) Whether the interference was in accordance with the law.
3) Whether there was a legitimate aim.
4) Whether the interference is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify the interference are relevant and sufficient. In determining this, the Court will consider the margin of appreciation that should be afforded to the underlying decision by national authorities.

1) Has there been an interference?

In considering whether there has been an interference, the Court will have due regard to:

1) The specific context in which the information at issue has been recorded and retained;
2) The nature of the records; and
3) The way in which these records are used and processed and the results that may be obtained.[214]

In general, the Court has adopted a broad approach to the question of whether or not there has been an interference. As set out in section 3, above, the protection of personal data is of fundamental importance to a person's enjoyment of the right to respect for private and family life and the collection, storage, alteration, disclosure, use and publication of information relating to an individual's private life can represent an interference with Article 8.

The Court has considered with interest the issues that storage and disclosure of cellular, DNA, fingerprint, photograph and voice recording data raise now and could raise in the future. The Grand Chamber in *S. and Marper v. the United Kingdom*,[215] held that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the question of whether there has been an interference. Bearing in mind the rapid pace of technological 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 precisely anticipated today.

2) Was any interference in accordance with the law?

The cases on the right to be forgotten have not turned to any significant extent on the question of whether any interference was "in accordance with the law". The Court has tended to find either that the interference was in accordance with the

[214] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §70.

[215] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04, 30566/04 at §§70-71 (included as a summary in this publication).

law or that this is more properly a question to be considered at justification stage. For example, in *Catt v. the United Kingdom*[216] the Court stated that the question of whether the collection, retention and use of the applicant's personal data was in accordance with the law is closely related to the broader issue of whether the interference was necessary in a democratic society. Therefore, the Court did not find it necessary to decide whether the interference was "in accordance with the law". The Court expressed the same view in *Gaughran*.[217]

3) Has the State asserted a legitimate aim?

On the question of legitimate aim, the Court has readily accepted the following aims as legitimate:

(a) The protection of national security.[218]
(b) The detection and prevention of crime and the safeguarding of the rights and freedoms of others.[219]
(c) The existence of a national register of sex offenders in order to prevent crime and combat recidivism, and also to make it easier to identify offenders.[220]
(d) The need for a comprehensive record of all cautions, convictions, warnings, reprimands, acquittals and other such information.[221] The Court made clear 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 circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed.[222]

[216] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §§106-107.

[217] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §73.

[218] *Segerstedt-Wiberg and Others v. Sweden*, judgment of 6 June 2006, no. 62332/00 at §87.

[219] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04, 30566/04 at §100 (included as a summary in this publication); *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §108

[220] *BB v. France*, judgment of 17 December 2009, no. 5335/06 at §58; *Gardel v. France*, judgment of 17 December 2009, no. 16428/05 at §63; and *MB v. France*, judgment of 17 December 2009, no. 22115/06 at §50.

[221] *MM v. the United Kingdom*, judgment of 13 November 2012, no. 24029/07 at §199.

[222] *MM v. the United Kingdom*, judgment of 13 November 2012, no. 24029/07 at §199.

(e) The need for a DNA database.[223] Again, the Court made clear that such facilities cannot be implemented as part of an abusive drive to maximise the information stored in them and the length of time for which they are kept. Without respect for the requisite proportionality vis-à-vis the legitimate aim 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.[224]

(f) The retention of biometric data and photographs for the purpose of detection and therefore, prevention of crime. The original taking of the 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 persons who may offend in future.[225]

4) Were measures taken by the State proportionate to the legitimate aim identified and justified?

The real battleground in the case law has been on the question of proportionality: is the interference proportionate to the legitimate aim pursued and are the reasons adduced by the national authorities to justify the interference relevant and sufficient? The test of proportionality is not whether or not another less restrictive regime could be imposed. The core issue is whether, in adopting the measures and striking the balance it did, the legislature acted within the margin of appreciation afforded to it.[226]

Margin of appreciation

First, as to the margin of appreciation, the Court has adopted the following approach in the context of cases in which the State holds information about an individual who has been subject to, or convicted following, investigation or judicial proceedings:

[223] *Aycaguer v. France*, judgment of 22 June 2017, no. 8806/12 at §34.

[224] *Aycaguer v. France*, judgment of 22 June 2017, no. 8806/12 at §34.

[225] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §75.

[226] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §95.

> "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. A margin of appreciation, the extent of which varies depending on a number of factors, including the nature of the activities restricted and the aims pursued by the restrictions, must therefore in principle be left to the States in this context. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted. Where, however, there is no consensus within the member states of the Council of Europe either as to the relative importance of the interest at stake or the best means of protecting it, the margin will be wider."[227]

Where a particularly important facet of an individual's existence or identity is at stake, the margin of appreciation accorded to a State will in general be restricted.[228]

The Court will consider broader state practice among member states when considering the extent of the margin of appreciation to be afforded to a State in a particular case. In *Gaughran*, in which the applicant alleged under Article 8 that the indefinite retention of his DNA profile, fingerprints and photograph in accordance with the blanket policy of retention of personal data of any individual convicted of a recordable offence amounted to a disproportionate interference, the Court held that there were a small number of States among those surveyed who operated indefinite retention regimes but the Court considered that those States were in a distinct minority.[229] The majority of States have regimes in which there is a defined limit on the period for which data can be retained. The Court could not conclude that the State's margin of appreciation was widened in the present case to the extent claimed by the Government. The United Kingdom was one of the few Council of Europe jurisdictions to permit indefinite retention of DNA profiles, fingerprints and photographs of convicted persons. The degree of consensus existing amongst Contracting States had narrowed the margin of appreciation available to the respondent State in particular in respect of the

[227] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §31.

[228] *Gardel v. France*, judgment of 17 December 2009, no. 16428/05 at §61.

[229] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §82 and 84.

retention of DNA profiles. The Court in *Gaughran* stressed the link between the margin of appreciation and the safeguards present in domestic systems to guard against abuse, stating that where a State has put itself at the limit of the margin of appreciation in allocating to itself the most extensive power of indefinite retention, the existence and functioning of certain safeguards becomes decisive.[230]

As to the margin of appreciation in the context of newspaper reporting the Grand Chamber in *Hurbain* stated that it had previously found that the margin of appreciation afforded to States in striking the balance between the competing rights is likely to be greater where news archives of past events, rather than news reporting of current affairs, are concerned.[231] In particular, 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 likely to be more stringent in the absence of any urgency in publishing the material. The Grand Chamber emphasised that these findings must be interpreted with due regard to the particular context of the case in question. The Grand Chamber stressed that it was of crucial importance that the Convention was interpreted and applied in a manner which rendered its rights practical and effective, not theoretical and illusory. A failure by the Court to maintain a dynamic and evolutive approach would risk rendering it a bar to reform or improvement.

Proportionality

The key considerations that have been taken into account by the Court when assessing the proportionality of measures that have been found to be an interference are addressed below under the four broad categories of individuals identified above:

1) Individuals investigated by police, or suspected or accused of committing an offence.
2) Individuals convicted of an offence.
3) Individuals in respect of whom security services collated and retained information.
4) Individuals who had been the subject of journalistic coverage as a result of investigation, arrest, or conviction.

[230] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §88.

[231] *Hurbain v. Belgium*, Grand Chamber judgment of 4 July 2023, no. 57292/16 at §181 (included as a summary in this publication).

Individuals investigated by police, or suspected or accused of committing an offence

(a) *Whether there is a pressing social need to collect the personal data*

For cases concerning individuals who have been investigated, suspected, or accused of committing an offence, the Court will consider whether there was a pressing social need to collect the data in question. In Catt, the applicant, a regular attender at public demonstrations, who had in the past been arrested but never convicted, complained that the retention of his data by the police was in violation of his right to privacy under Article 8. The Court acknowledged the need for data collection particularly in the context of individuals who are part of protest groups known to be violent and set out how to consider a "pressing social need".[232] The Court stated that the question for it to examine was not whether there was a "pressing social need" for the police to establish and maintain such a database. To the extent that the Court examines this issue from a more general aspect, it had done so in its conclusion that the creation of the database pursued a legitimate aim. At this stage, the Court was examining whether the collection and retention of the applicant's personal data may be regarded as justified under the Convention. The Court accepted that there was a pressing need to collect the personal data about the applicant. It agreed with the UK Supreme Court that it is in the nature of intelligence gathering that the police will first need to collect the data, before evaluating its value. In this respect, the Court recalled that the personal data in question was overtly obtained. The Court also agreed that the police had an obvious role to monitor protests where the activities of that group were known to be violent and potentially criminal. Even if the applicant himself was not suspected of being directly involved in a group's criminal activities, it was justifiable for the police to collect his personal data as he had decided to repeatedly and publicly align himself with the activities of a violent protest group.

(b) *Whether there is a pressing social need to retain the data*

While the Court in Catt found that there was a need to collect data, the Court had a different view on the question of whether that data needed to be retained. In Catt, the Court also held that there was not a pressing need to retain the applicant's data.[233] It shared the domestic court's concern that there was a need

[232] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §§116-118.

[233] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §§119 and 124.

for caution before overriding the police's judgement about what information is likely to assist them in their task. The Court underlined that its conclusion did not call into question the fact that there may have been a pressing need for the police to retain the applicant's personal data for a period of time after it was collected. However, in the absence of any rules setting a definitive maximum time limit the applicant was entirely reliant on the diligent application of the highly flexible safeguards to ensure the proportionate retention of his data. The Court held that where a State chooses to put in place such a system, the necessity of effective procedural safeguards becomes decisive. Those safeguards must enable the deletion of any such data once its continued retention becomes disproportionate. Principle 2 on the collection of data in Recommendation R (87) 15 states that the collection of data on individuals solely on the basis that they belong to particular movements or organisations which are not proscribed by law should be prohibited unless absolutely necessary or for the purposes of a particular inquiry. The Court considered that the retention of the applicant's data in particular concerning peaceful protest had neither been shown to be absolutely necessary, nor for the purposes of a particular inquiry.

(c) *The need for safeguards*

The Court is cognisant of the need for safeguards to be present in domestic law whenever State authorities retain or disclose information about individuals. In *MK v. France*, in which the applicant alleged a violation of Article 8 on the grounds of the retention of data relating to him in the national fingerprint database, the Court held that the need for safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data is used for police purposes.[234] The domestic law should notably ensure that such data is relevant and not excessive in relation to the purposes for which it is stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse.

In *Catt*, the Court found that the absence of effective safeguards was of particular concern as personal data revealing political opinions attracts a heightened level of protection.[235] The Court held that engaging in peaceful protest

[234] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §32.

[235] *Catt v. the United Kingdom*, judgment of 24 January 2019, no. 43514/15 at §123.

has specific protection under Article 11 of the Convention, which also contains special protection for trade unions, whose events the applicant attended. In this connection, it noted that in the National Coordinator's statement, the definition of "domestic extremism" referred to collection of data on groups and individuals who act "outside the democratic process". Therefore, the police did not appear to have respected their own definition in retaining data on the applicant's association with peaceful, political events. Such events are a vital part of the democratic process. The Court had already highlighted the danger of an ambiguous approach to the scope of data collection in the present case. It considered that the decisions to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that, in the circumstances, its retention must have had a chilling effect.

(d) *The need to ensure that the State's arguments are not tantamount to justifying the storage of information on the whole population*

While the Court has accepted a broad range of aims as "legitimate" in principle, the Court has carefully considered the measures actually taken by State authorities in pursuit of those aims, including whether the measures are excessively wide-ranging in scope. In *MK v. France*, the applicant alleged a violation of Article 8 on the grounds of the retention of data relating to him in the national fingerprint database. The Government alleged, *inter alia*, that retention of the data would protect the applicant's interests by ruling out his involvement should someone attempt to steal his identity. The Court set out that besides the fact that such a reason is not explicitly mentioned in the domestic provisions, accepting this argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant.[236]

(e) *The length of time for retention, whether this is tantamount to indefinite retention, and whether there is a real ability for an applicant to apply for deletion of data*

Where State authorities allege that measures taken have been proportionate because the retention of information is time limited, or an applicant can apply for deletion of the information, the Court will prioritise substance over form, and

[236] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §37.

consider the practice which actually occurs at domestic level. In *MK v. France*, the Court held that in that case, the right at any time to submit a deletion request to the court was liable to conflict with the interests of the investigating authorities, which were said to require access to a database with as many references as possible.[237] Since the interests at stake were contradictory, if only partially, the deletion, which was not in fact a right, provided a safeguard which was "theoretical and illusory" rather than "practical and effective". The Court noted that while the retention of information stored in the file was limited in time, it extended to 25 years. Having regard to its previous finding that the chances of deletion requests succeeding were at best hypothetical, a 25-year time-limit was in practice tantamount to indefinite retention, or at least, as the applicant contended, a standard period rather than a maximum one.

Similarly, in *Brunet v. France*,[238] a case concerning a complaint about the applicant's details being recorded in a crime database after the discontinuance of criminal proceedings against him, the Court found that the applicant had not had a real possibility of seeking the deletion from the database of information concerning him and that the length of retention of that data, 20 years, could be assimilated if not to indefinite retention, at least to a norm rather than to a maximum legal limit. The Court concluded that there had been a violation of Article 8.

(f) *The need to consider the gravity of the offence in issue*

The gravity of the offence in issue will be relevant in the Court's assessment of the proportionality of measures collecting or retaining personal information. In *MK v. France*, the Court concluded that the respondent State had overstepped its margin of appreciation as the regulations on the retention in the impugned database of the fingerprints of persons suspected of having committed offences but not convicted, as applied to the applicant, did not strike a fair balance between the competing public and private interests at stake. Consequently, the retention of the data had to be seen as a disproportionate interference with the applicant's right to respect for private life and could not be regarded as necessary in a democratic society.

In so finding, the Court held that in addition to the primary function of the database (which was to facilitate efforts to find and identify the perpetrators

[237] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §§41-42.

[238] *Brunet v. France*, judgment of 18 September 2014, no. 21010/10.

of serious crimes and other major offences) the decree in question mentioned another function, namely, to facilitate "*the prosecution, investigation and trial of cases referred to the judicial authority*", without specifying whether this was confined to serious crimes and other major offences.[239] It also covered "*persons who have been charged in criminal proceedings and whose identification is required*", and so could embrace all offences *de facto*, including mere summary offences, if, in theory, this would help identify the perpetrators of crimes and offences as specified in the decree. The circumstances of the case, which concerned book theft and was discontinued, showed that the instrument applied to minor offences. The case was thus very different from those specifically relating to serious offences such as organised crime[240] or sexual assault.[241]

(g) *The need to draw distinctions between accused individuals and convicted individuals*

The Court recognises that the position of an accused and a convicted person should be treated differently. One criticism by the Court in ***MK v. France*** was that the decree in question drew no distinction between whether or not the person concerned had been convicted by a court or even prosecuted.[242]

(h) *The risk of stigmatisation of people who are merely accused*

The Court has recognised that the retention of the data of people who have merely been investigated or accused of an offence, not convicted, can nevertheless lead to stigmatisation, or an assumption that the individual is indeed culpable of an offence. In *S. and Marper*, the Court set out its concern of stigmatisation stemming from the fact that persons in the position of the applicants, who had not been convicted of any offence and were entitled to the presumption of innocence, were treated the same way as convicted persons.[243] The Court stressed the right of every person to be presumed innocent and that this included the general

[239] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §41.

[240] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 (included as a summary in this publication).

[241] *BB v. France*, judgment of 17 December 2009, no. 5335/06; *Gardel v. France*, judgment of 17 December 2009, no. 16428/05; and MB v. France, judgment of 17 December 2009, no. 22115/06.

[242] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §42.

[243] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 at §§122-123 (included as a summary in this publication).

rule that no suspicion regarding an accused's innocence may be voiced after his acquittal. It was true that the retention of the applicants' private data could not be equated with the voicing of suspicions. However, the Court considered that the applicants' perception that they were not being treated as innocent was heightened by the fact that their data was to be 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 was required to be destroyed. The Court stated that weighty reasons would have to be put forward by the State before the Court could regard as justified such a difference in treatment of the applicants' private data compared to that of other people who had not been convicted. Likewise, in MK v. France the Court stated that the conditions of retention of the data must not give the impression that the persons concerned are not being treated as innocent.[244]

(i) *The risk of harm to minors*

The Court acknowledges that the retention of data in respect of minor children can affect their long-term ability to be rehabilitated and to integrate within society. The Court addressed this in *S. and Marper*, stating that the retention of data of persons who had been suspected, but not convicted, may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society.[245] The Court cited Article 40 of the UN Convention on the Rights of the Child, and noted the special position of minors in the criminal-justice sphere. It noted, in particular, the need for the protection of their privacy in criminal trials. The Court considered that particular attention should be paid to the protection of juveniles from any detriment that may result from the retention by the authorities of their private data following acquittals of a criminal offence. The Court shared the view of the Nuffield Council on Bioethics as to the impact on young persons of the indefinite retention of their DNA material and noted the Council's concerns that the policies applied had led to the over-representation in the database of young persons and ethnic minorities who had not been convicted of any crime.

[244] *MK v. France*, judgment of 18 April 2013, no. 19522/09 at §33.

[245] *S. and Marper v. the United Kingdom*, Grand Chamber judgment of 4 December 2008, nos. 30562/04 and 30566/04 at §124 (included as a summary in this publication).

Individuals convicted of an offence

Similar issues as with accused individuals have arisen in respect of individuals who have been convicted of offences.

(a) *The need for safeguards*

The Court has stressed the need for safeguards in cases concerning information held or disseminated about individuals who have been convicted of an offence. In *Gardel* the Court held that the need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data is being used for police purposes.[246] The domestic law should notably ensure that such data is relevant and not excessive in relation to the purposes for which it is stored and that it is preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored. The domestic law must also afford adequate guarantees to ensure that retained personal data is efficiently protected from misuse and abuse.[247]

In *MM v. United Kingdom*,[248] the applicant had complained about the retention and disclosure in the context of a criminal record check of data concerning a caution she received from the police. Her complaint had been lodged following the withdrawal of an offer of employment which had been made to her after she had disclosed the existence of a caution. In the course of finding a violation of Article 8, the Court considered the potential adverse effect on individuals who are applying for employment of the retention of data on minor offences or offences of questionable relevance. The Court stated 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. The obligation on the authorities responsible for retaining and disclosing criminal record data to secure respect for private life was particularly important, given the nature of the data held and the potentially devastating consequences of their disclosure. Even where the criminal record certificate records a conviction or a caution for a relatively minor, or questionably relevant, offence, a prospective employer may well feel it safer to reject the applicant. The Court agreed that it is realistic to assume

[246] *Gardel v. France*, judgment of 17 December 2009, no. 16428/05 at §62.

[247] *Aycaguer v. France*, judgment of 22 June 2017, no. 8806/12 at §38.

[248] *MM v. the United Kingdom*, judgment of 13 November 2012, no. 24029/07.

that, in the majority of cases, an adverse criminal record certificate will represent something close to a "*killer blow*" to the hopes of a person who aspires to any post which falls within the scope of the disclosure requirements.

The Court highlighted the absence of a clear legislative framework for the collection and storage of data, and the lack of clarity as to the scope, extent and restrictions of the common law powers of the police to retain and disclose caution data. It referred to the absence of any mechanism for independent review of a decision to retain or disclose data. Finally, the Court noted the limited filtering arrangements in respect of disclosures made. No distinction was made on the basis of the nature of the offence, the disposal in the case, the time which had elapsed since the offence took place, or the relevance of the data in the employment sought.

The cumulative effect of these shortcomings was that the Court was not satisfied that there were sufficient safeguards in the system for the retention and disclosure of criminal record data to ensure that data relating to the applicant's private life had not been, and would not be, disclosed in violation of her right to respect for her private life.[249]

(b) *The need to ensure that the State's arguments are not tantamount to justifying the storage of information on the whole population*

As for MK v. France above in respect of accused people, in *Gaughran*, in response to the Government's assertion that the more data that is retained, the more crime is prevented, the Court emphasised that accepting such an argument in the context of a scheme of indefinite retention 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.[250]

(c) *The length of time for retention, whether this is tantamount to indefinite retention, and whether there is a real ability for an applicant to apply for deletion of data*

As is the case for accused persons, the Court will consider in cases involving convicted persons whether retention of information is time limited and whether

[249] *MM v. the United Kingdom*, judgment of 13 November 2012, no. 24029/07 at §§200 and 206-207.

[250] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §89.

the individual can apply for deletion of the information. In *Gardel*, a case concerning the entry of the applicant's name on to a national judicial database of sex offenders, the Court held that the period of time for which data was kept was not disproportionate to the aim pursued in storing the information and the individual had a practical opportunity to apply for deletion of the data.[251] The Court considered that the judicial procedure for the removal of data provided for independent review of the justification for retention of the information according to defined criteria and afforded adequate and effective safeguards of the right to respect for private life having regard to the seriousness of offences giving rise to placement on the register. The storing of the data for such a long period could give rise to an issue under Article 8. However, the Court noted that the applicant would in any event have a practical opportunity to lodge an application for removal of the stored data from the date on which the decision giving rise to the data's entry in the register ceased to have effect. In these circumstances, the Court considered that the period of time for which the data was kept was not disproportionate to the aim pursued in storing the information. The cases of *BB v. France* and *MB v. France* had similar underlying facts to *Gardel*. The Court found no violation of Article 8 in any of these cases.

In contrast, in *Aycaguer*, there was no provision for the deletion of data of convicted persons. In finding a violation of Article 8, the Court held that the 40-year period in principle constituted a maximum which should have been adjusted under a separate decree.[252] Since no such decree has ever been issued, the 40-year period was in practice, treated as indefinite storage, or at least as a norm rather than a maximum. As regards to the deletion procedure, it was not disputed that access to such a procedure was only authorised for suspects, and not for convicted persons such as the applicant. The Court considered that convicted persons should also be given a practical means of lodging a request for the deletion of registered data. That remedy should be made available in order to ensure that the data storage period is proportionate to the nature of the offences and the aims of the restrictions.

In *Gaughran*[253], the Court found that in practice there was no ability for an individual to have his or her data deleted. The applicant's biometric data and photographs were retained without reference to the seriousness of his offence

[251] *Gardel v. France*, judgment of 17 December 2009, no. 16428/05 at §69.

[252] *Aycaguer v. France*, judgment of 22 June 2017, no. 8806/12 at §34.

[253] *Gaughran v. the United Kingdom*, judgment of 13 February 2020, no. 45245/15 at §94.

and without any regard to any continuing need to retain that data indefinitely. The police were vested with the power to delete biometric data and photographs only in exceptional circumstances. 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. Accordingly, the review available to the individual appeared to be so narrow as to be almost hypothetical.

(d) *The need to consider the gravity of the offence in issue*

The gravity of the offence in issue will be relevant to the Court's assessment of the proportionality of measures collecting or retaining personal information about convicted individuals. In *Aycaguer* at the Court noted that the Constitutional Council had issued a decision to the effect that the provisions relating to the impugned computer file were in conformity with the Constitution, subject inter alia to "*determining the duration of storage of such personal data depending on the purpose of the file stored and the nature and/or seriousness of the offence in question*."[254] However, no appropriate action had been taken on that reservation. No differentiation was provided for based on the nature and/or seriousness of the offence committed, notwithstanding the significant disparity in the situations that could arise. The applicant's situation demonstrated this, with events occurring in a political/trade union context, concerning mere blows with an umbrella directed at police officers who had not even been identified. This was in contrast to the seriousness of the acts liable to constitute the very serious offences set out in domestic law such as sex offences, terrorism, crimes against humanity, and trafficking in human beings. The Court noted that the *Aycaguer* case was very different from cases relating to such serious offences as organised crime or sexual assault.

(e) *The importance of rehabilitation*

The Court also has considered the development of European penal policy in respect of adults, and how this includes the aim of rehabilitation. The retention of data, and its accessibility by the public, can impede an individual's rehabilitation and reintegration into society. The Court emphasised in *Gardel*, that European penal policy is evolving and attaching increasing importance, alongside the aim of

[254] *Aycaguer v. France*, judgment of 22 June 2017, no. 8806/12 at §43.

punishment, to the rehabilitative aim of imprisonment, particularly towards the end of a long prison sentence.[255] Successful rehabilitation means, among other things, preventing reoffending.

(f) *The accessibility of the information*

The Court will consider how accessible information held about individuals is to the public, and for which purposes it may be used. In *Gardel*, in which the applicant complained of his placement on the national register of sex offenders following his conviction, the responsible way in which information was stored contributed to a finding of no violation of Article 8. The rules on access to the register meant that it could only be consulted by judicial authorities, the police and administrative bodies that were bound by a duty of confidentiality, and in precisely defined circumstances.[256]

Individuals in respect of whom security services have collated and retained information

In *Segerstedt-Wiberg*, the Court held that powers of secret surveillance are tolerable under the Convention only so far as strictly necessary for the safeguarding of democratic institutions.[257] Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued. In that case, in view of the nature and age of the information on certain of the applicants, the reasons behind the storage of the data, although relevant, could not be deemed sufficient 30 years later.

Individuals who had been the subject of journalistic coverage as a result of investigation, arrest, or conviction.

The Grand Chamber in *Hurbain* has addressed at length the right to be forgotten in the context of information about an individual's investigation, arrest or conviction that has been published and stored by journalists or newspapers. The applicant argued that the civil judgment ordering him to anonymise an online, archived article that mentioned the full name of the driver (G) responsible for an historic fatal road-traffic accident, violated his rights under Article 10. The

[255] *Gardel v. France*, judgment of 17 December 2009, no. 16428/05 at §64.

[256] *Gardel v. France*, judgment of 17 December 2009, no. 16428/05 at §70.

[257] *Segerstedt-Wiberg and Others v. Sweden*, judgment of 6 June 2006, no. 62332/00 at §§88-92.

Grand Chamber found there to be no violation. The Court had hitherto not upheld any measure removing or altering information published lawfully for journalistic purposes and archived on the website of a news outlet.

No issues arose as to whether or not there was an interference, a legal basis or a legitimate aim (here, the protection of the reputation or rights of others in respect of G). The only question was that of proportionality and justification. The Court considered previous cases, including that of *ML and WW v. Germany*[258] and *Biancardi v. Italy*[259].

1) *ML and WW* concerned the refusal of the domestic court to order three different media organisations to anonymise press files concerning the applicants' conviction for the murder of a well-known actor, in which the applicants were referred to by their full names. In finding that there had been no violation of Article 8 in respect of the applicants, the Court had regard to the following considerations: the fact that at the time that the applicants' requests for anonymisation were lodged the impugned reports had continued to contribute to a debate of public interest; the fact that the applicants were not simply private individuals unknown to the public; the applicants' conduct with regard to the media, which they had approached after their conviction with a view to having the proceedings reopened; the fact that the reports had relayed the facts in an objective manner and without the intention to present the applicants in a disparaging way or to harm their reputation; and the limited accessibility of the information. In *ML and WW*, the Court noted that the risk of harm posed by content on the Internet was higher than that posed by the press on account of the important role of search engines.[260] The Court also stated that the ease with which information can be found on the Internet creates an amplifying effect on the dissemination of information and the nature of the activity underlying the publication of information, so the obligations of search engines towards an individual who is the subject of information may differ from those of the entity which originally published the information.[261] The balancing of the interests at stake could result in different outcomes depending on

[258] *ML and WW v. Germany*, judgment of 28 June 2018, nos. 60798/10 and 65599/10.

[259] *Biancardi v. Italy*, judgment of 25 November 2021, no. 77419/16 (included as a summary in this publication).

[260] *ML and WW v. Germany*, judgment of 28 June 2018, nos. 60798/10 and 65599/10 at §91.

[261] *ML and WW v. Germany*, judgment of 28 June 2018, nos. 60798/10 and 65599/10 at §97.

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 facilitating identification of any available information on that person and establishing a profile on them.

2) In *Biancardi*,[262] the applicant, the former editor-in-chief of an online newspaper, was held liable in civil law for having kept on his newspaper's website an article from 2008 reporting on a fight in a restaurant and giving details of the criminal proceedings opened in that connection. The Court found that not only Internet search engine providers but also the administrators of newspaper or journalistic archives accessible through the Internet, such as the applicant, could be required to de-index documents. The Court found there to be an interference with the applicant's right to impart information but that there was a legitimate aim – the protection of the restaurant owner's reputation, and the interference had been necessary. In arriving at that conclusion, the Court took into consideration the following criteria: the length of time for which the article was kept online, the sensitiveness of the data and the gravity of the sanction imposed (a civil fine rather than a requirement to remove the article).[263] It ruled that there had been no breach of the applicant's freedom of expression especially since he had not actually been required to remove the article from the website.

The key reasoning of the Grand Chamber in *Hurbain* is at paragraphs 201 to 211 of the judgment. The Court's assessment took account of the different context of the case, being digital archives, compared with cases concerning initial publication. Regard being had to the general principles referred to above, in particular to the need to preserve the integrity of press archives, and also, to some extent, to the practice of the courts in the Council of Europe member States, the Court considered that the balancing of these various rights of equal value in the context of a request to alter journalistic content that is archived online should take into account the following criteria:

[262] *Biancardi v. Italy*, judgment of 25 November 2021, no. 77419/16 (included as a summary in this publication).

[263] *Biancardi v. Italy*, judgment of 25 November 2021, no. 77419/16 at §§62-69 (included as a summary in this publication).

i) The nature of the archived information;
ii) The time that has elapsed since the events and since the initial online publication;
iii) The contemporary interest of the information;
iv) Whether the person claiming entitlement to be forgotten is well known and his or her conduct since the events;
v) The negative repercussions of the continued availability of the information online;
vi) The degree of accessibility of the information in the digital archives; and
vii) The impact of the measure on freedom of expression and more specifically on freedom of press.

The Grand Chamber found that in order for Article 8 to come into play, an attack on a person's reputation must attain a certain level of seriousness. In most instances, several criteria will need to be taken into account simultaneously in order to determine the protection to be afforded to private life when set against the other interests at stake and against the means employed to give effect to that protection in a particular case.

Data subjects are not obliged to contact the original website in order to exercise their right vis-à-vis search engines, as the processing by search engines and that of the original website are two different forms of processing, each with its own grounds of legitimacy and with different impacts on the individual's rights and interests. Likewise, the examination of an action against the publisher of a news website cannot be made contingent on a prior request to a search engine for delisting. In the Court's view, this distinction between the activities of search engine operators and those of news publishers retains its significance when the Court is examining any interference with freedom of expression, including the public's right to receive information, based on a claim of entitlement to be forgotten.

The Court acknowledged that the chilling effect on freedom of the press stemming from the obligation for a publisher to anonymise an article that was initially published in a lawful manner cannot be ignored. The obligation to review at a later stage the lawfulness of the continued online availability of an article following a request from a person claiming to be a victim of the situation entails a risk that the press may refrain in future from keeping reports in online archives, or that it will omit individualised elements in articles that are likely to be the subject of such a request. Nevertheless, content providers are required to assess and

weigh up the interests in terms of freedom of expression and respect for private life only where the person concerned makes an express request to that effect.

Although in the context of a balancing exercise between the right to freedom of expression and the right to respect for private life these two rights are to be regarded as being of equal value, it does not follow that the criteria to be applied in conducting that exercise all carry the same weight. In this context, in fact, the principle of preservation of the integrity of press archives must be upheld, which implies ensuring that the alteration and, *a fortiori*, the removal of archived content is limited to what is strictly necessary, so as to prevent any chilling effect such measures have on the performance by the press of its task of imparting information and maintaining archives. Hence, in applying the above-mentioned criteria, particular attention should be paid to properly balancing, on the one hand, the interests of the individuals requesting the alteration or removal of an article concerning them in the press archives and, on the other hand, the impact of such requests on the news publishers concerned and also, as the case may be, on the functioning of the press.

In conclusion, the Court found that the national courts took account in a coherent manner the nature and seriousness of the judicial facts reported on in the article in question, the fact that the article had no topical, historical or scientific interest, and the fact that G. was not well known. In addition, they attached importance to the serious harm suffered by G. as a result of the continued online availability of the article with unrestricted access which was apt to create a "virtual criminal record" especially in view of the length of time that had elapsed since original publication. Further, after reviewing the measures that might be considered in order to balance the rights at stake, the national courts had held that the anonymisation of the article did not impose an excessive and impracticable burden on the applicant, while constituting the most effective means of protecting G.'s privacy. In these circumstances, and regard being had to the margin of appreciation, the Court found that the national courts had carefully balanced the rights at stake such that the interference with Article 10 was limited to what was strictly necessary and thus, could be regarded as necessary in a democratic society and proportionate. It found no strong reasons to substitute its own view. Accordingly, there was no violation of Article 10.

Chapter 6

Conclusion

This area of data protection and the right to be forgotten, in the context of investigative and judicial proceedings, is ever evolving due to the fast-paced developments in modern technology. The Court is aware of the difficulties that this can present and the need for balancing competing rights now, with a view to how data could be put to different use even in the near future.

The Court has shown willingness to define "personal data" in a broad sense, to encompass information which directly and indirectly identifies an individual. The fact that data is in the public domain does not mean it loses its "personal" quality. The Court will also treat certain categories of data as more "sensitive" and require a heightened degree of protection for that data, acknowledging that disclosure of such data can dramatically affect an individual's private and family life, social and employment situation and expose them to the risk of ostracization.

The Court has protected data during the investigative stages of proceedings and stressed the importance of doing so. This is a rapidly changing area in which States are using methods of intercepting communications for the prevention of crime and the maintenance of security, and at the same time, individuals and groups are finding communication tools which specifically aim to protect private communications from interception. As set out above, it is not yet clear whether the collection, storage and transfer of data from EncroChat, Anom and Sky ECC will constitute a breach of Article 8. As to the use of any such material in judicial proceedings, it will be relevant the extent to which an individual's defence can challenge and examine the authenticity and reliability of any such evidence. States must exercise extra vigilance if using evidence obtained in another jurisdiction in which safeguards surrounding gathering evidence may be different.

In the context of publishing information about judicial proceedings, States must navigate a balance between considerations of open justice and data

protection, all the while bearing in mind the importance of the presumption of innocence under Article 6.

The right to be forgotten is of ever-increasing importance to individuals. Technology and society's use of technology has progressed so that news articles about offences committed by an individual come up at the first-click of a search button decades later. This can have a severe impact on that individual's personal and professional relationships. The Court has recognised that even accusations against individuals can lead to the permanent questioning of their character. The ability of the DNA of an individual to be held forever and be linked to his or descendants also throws up ethical questions pitting the prevention of crime and the maintenance of national security against the privacy of an individual and potentially, their family members. The tensions between Article 8 and Article 10 will continue to arise in different contexts, and domestic judges must ensure they have turned their minds to all relevant considerations before coming down on the side of privacy or free expression.

Governments, lawyers, State judiciaries, and the NGO sector will all need continuing education to understand how newly developing technologies can and could affect individuals' long-held rights and to meet the challenges posed as a result. A careful, nuanced consideration of all competing rights in issue will be essential in complying with the requirements of the Convention in this fascinating area.

PART 2

Case Summaries:

The lawful and proportionate disclosure of an intercepted conversation with the Prime Minister, regarding a matter of public interest, did not violate Article 8 in spite of reputational impact

JUDGMENT IN THE CASE OF
ALGIRDAS BUTKEVIČIUS v. LITHUANIA

(Application no. 70489/17)
14 June 2022

1. Principal facts

The applicant was born in 1958 and lived in Vilnius. He had been a member of the Seimas (Lithuanian Parliament) since 1996; at the time of the case, he was the Prime Minister of Lithuania, a post in which he served from November 2012 to November 2016.

In 2015, a regional prosecutor's office and the Special Investigations Service of Lithuania were conducting a pre-trial investigation into alleged political corruption related to the passage of a certain government resolution. The government resolution would have impacted territories' "resort" status and privileges; it was adopted in September 2015 and later annulled in May 2016. In the course of this investigation, a court had authorised recording of the phone calls of a local politician (R.M.), mayor of a resort territory. One of the telephone conversations intercepted in the course of the investigation was between the applicant and R.M. During this conversation, the government resolution was briefly discussed.

The regional prosecutor eventually decided to discontinue the pre-trial investigation, as no crimes had apparently been committed. The discontinuation decision contained transcripts of the telephone conversation between the

applicant and R.M. Separately, the Seimas Anti-Corruption Commission ("the Commission") was instructed to conduct a parliamentary inquiry into the adoption of the government resolution. In the course of their inquiry, the regional prosecutor sent the Commission a copy of the discontinuation decision, including the phone call transcripts. The Commission eventually held a public hearing on the matter, during which the pre-trial investigation was discussed.

One of the journalists present at the public hearing later published an online article, headlined "Juicy details in the conversations that were made public", in which selected extracts from the applicant's telephone call transcripts appeared in a light negative to the applicant. Based upon this initial disclosure, the transcript excerpts were subsequently widely reported upon. The applicant issued a complaint with the General Prosecutor's Office, and later with the domestic courts, as to the public disclosure of the telephone conversation and its interference with his Article 8 right to respect for private and family life, but these efforts were unsuccessful.

2. Decision of the Court

The applicant complained that the public release of his correspondence demonstrated a failure on the part of the State to adequately protect his privacy, and that it had weighed heavily on his private life, in breach of his Article 8 rights.

Article 8

The Court emphasised that private conversations and correspondence, whatever their content and wherever they take place, are protected under Article 8, without express or implied qualification. This may be extended to include professional activities, which are often difficult or impossible to isolate from an individual's private life and identity, including their private relationships. Therefore, the Court found that Article 8 was applicable to the applicant's circumstances.

The Court further acknowledged that the transmission of the applicant's intercepted phone conversation, and the examination of the conversation transcripts at the Commission's public hearing, had constituted an interference with the applicant's rights under Article 8.

The applicant did not contest the fact that the stated interference with his private life had been executed lawfully; he instead complained that the prosecutor's transfer of the transcripts, and the lack of restrictions on public access, constituted a

failure to protect his private life. Given that the conversation in question concerned possible political corruption and illegal activity, the Court determined that the regional prosecutor had not only a right, but an obligation to send the transcripts to the Chief Official Ethics Commission. The regional prosecutor had therefore acted in compliance with standard domestic law and procedure.

Domestic authorities had concluded that the prosecutor had not breached any rules or ethics standards in criminal proceedings by releasing the transcripts; further, domestic courts had never seen fit to quash the prosecutor's findings. Finally, the transcript had been disclosed within the Commission's standard framework, as regulated by domestic law. In deference to the remit, judgement, and procedures of local authorities, and in absence of any clear evidence of arbitrariness on their part, the Court therefore rejected the applicant's argument that the State had failed to sufficiently protect the information it had gathered during the pre-trial investigation.

The legal basis of the State's interference was both accessible and foreseeable. Specifically, the applicant should have foreseen that his actions were subject to public scrutiny, given his official role, and that legal authorities' obligations to promote political transparency further undermined the applicant's claims to privacy. For all these reasons, it was in accordance with the law.

In the applicant's case, the interference had been in pursuit of legitimate aims, including the protection of the rights and freedoms of others, accountability for corruption, and crime prevention. Further, the correspondence was concerning a political matter, and did not include sensitive information about the applicant's private life, such as information about his health or sexual life.

The Court then asked whether the interference had been necessary in a democratic society. It emphasised the importance of balancing the competing interests presented by the applicant's case, such as the applicant's right to honour and reputation, the right of the press to report on matters of public interest and concern; the right of the public to access such information and to political transparency; and limitations on public individuals' expectation to privacy whilst operating in an official capacity. Not only are public figures not entitled to total privacy, matters of a public nature are as a general rule protected by Article 8. Indeed, the private lives of public figures may be a matter of popular interest, and may implicate others' rights and freedoms.

The Court acknowledged that the interference had affected the applicant's private life, and in particular his reputation; it further conceded that reputational concerns can be particularly impactful for public figures and politicians. However, in contrast to other cases involving interference with Article 8 rights in professional settings, the applicant had not experienced any measurable, tangible repercussions beyond some loss of reputation. In addition, the government resolution at issue in the applicant's telephone call and during the pre-trial investigation had subsequently been annulled, so any associated stigma surrounding the matter had been legally put to rest.

The Court was therefore unable to conclude that the interference had been disproportionate to the legitimate aims pursued. The Court found that there had been no violation.

The exclusion of a public hearing and a public pronouncement of judgment in child residence proceedings did not violate Article 6 § 1 of the Convention

JUDGMENT IN THE CASE OF
B. AND P. v. UNITED KINGDOM

(Application nos. 36337/97 and 35974/97)
24 April 2001

1. Principal facts

The applicants were born in 1963 and 1949 and lived in the United Kingdom. Both applicants had instituted proceedings in the UK County Court for residence orders under section 8(1) of the Children Act 1989 (the Act) in relation to their respective sons, following separation from their partner or wife (the residence applications).

Both applicants asked for their applications to be heard in a public hearing and for the judgments to be pronounced in public. These requests were refused. The relevant domestic rule in respect of proceedings under the Act provided that "unless the court otherwise directs, a hearing of, or directions appointment in, proceedings to which this Part applies shall be in chambers". The Court of Appeal dismissed the applicants' appeals against the judges' decisions on the basis that the respective judges had properly exercised their discretion in refusing to hear the applications in open court and in making anonymity orders.

B's case was held in chambers (in private) throughout. P's case was also held in chambers, although his second application for custody was heard in open court. In respect of B, the judge dealing with the case ordered that no documents used in the proceedings should be disclosed outside the court. B also alleged that the judge warned him that any publication of information obtained in the context of the proceedings would amount to contempt of court for which B could be sent to prison. Both applicants' residence applications were dismissed by the County Court. The judgments in both proceedings were pronounced in chambers, and the parties were provided with a copy of the judgment in writing.

2. Decision of the Court

The applicants complained that the fact that their cases were not heard in public and that the judgments were not publicly announced violated their rights under Article 6 § 1 of the Convention (right to a fair and public hearing). They further complained that the bar on disclosing any information about the proceedings violated their rights under Article 10.

Article 6

Considering first the complaint in relation to the lack of a public hearing, the Court noted its case law on the importance of the public character of proceedings in achieving the aim of a fair hearing under Article 6 § 1. However, the requirement to hold a public hearing is subject to exceptions. The Court considered that the child residence proceedings were prime examples of cases where the exclusion of the press and public may be justified in order to protect the privacy of the child and parties and to avoid prejudicing the interests of justice. For the judge to be able to gain as full and accurate a picture as possible of the advantages and disadvantages of the various residence and contact options, it was essential that the parents and other witnesses felt able to express themselves candidly without fear of public curiosity or comment.

Although the Court recognised that Article 6 § 1 states that as a general rule civil proceedings should take place in public, it was not inconsistent with this for a State to designate an entire class of case as an exception to the general rule, where considered necessary for a legitimate aim. The domestic procedural rule was a specific reflection of the general exceptions provided for by Article 6 § 1. The domestic courts also had a discretion to hold proceedings in public if merited by the special features of the case, and a judge had to consider whether to exercise this discretion if requested by one of the parties.

In respect of the first applicant, although the first instance judge appeared to consider he had no power to order the hearing to take place in public, this misstatement of the domestic law was corrected on appeal, and the judge had later explained that a public hearing was not in the child's interests. In respect of the second applicant, the judges at first instance and on appeal had given careful consideration and detailed explanations of their reasons. Accordingly, the Court did not consider that there was any violation of Article 6 § 1 in respect of the lack of public hearing.

As regards the refusal of the domestic courts to publicly pronounce their judgments on the residence applications, the Court recalled its long-standing case law that the form of publicity given under the domestic law to a judgment must be assessed in light of the special features of the proceedings in question and by reference to the object and purpose of Article 6 § 1.

The Court noted its conclusion that the domestic authorities were justified in conducting proceedings in private in order to protect the privacy of the children and the parties and to avoid prejudicing the interests of justice. The Court considered that to pronounce the judgment in public would, to a large extent, frustrate these aims.

Further, the Court noted that anyone who can establish an interest could consult or obtain a copy of the full text of the orders and/or judgments, and the judgments of the Court of Appeal and of the first instance courts in cases of special interest were routinely published. The public were therefore able to study the manner in which the courts generally approached child residence cases and the principles applied in deciding them.

A literal interpretation of the terms of Article 6 §1 concerning the pronouncement of judgments would not only have been unnecessary for the purpose of public scrutiny, but it might have frustrated the primary aim of Article 6 to secure a fair hearing.

The Court accordingly concluded that Article 6 §1 did not require the judgments in the cases to be public.

Article 10

In view of its findings on Article 6, the Court concluded that it was not necessary to examine separately the applicants' complaints under Article 10.

Civil sanctioning of an editor for lengthy refusal to de-index article on a criminal case against private persons did not violate the editor's Article 10 rights

JUDGMENT IN THE CASE OF
BIANCARDI v. ITALY

(Application no. 77419/16)
25 November 2021

1. Principal facts

The applicant was an Italian national who was born in 1972 and lived in Pescara. He was editor-in-chief of an online newspaper.

In March 2008, he published an article concerning a fight involving a stabbing in a restaurant. The article mentioned the names of those involved, namely the family, two brothers, and their respective sons, who owned the restaurant. It also reported that the reason for the fight had probably been related to a financial quarrel over ownership of a building and gave details about the family members' house arrest and/or detention.

In September 2010, one of the brothers and his restaurant sent a formal notice to the applicant asking that the article be removed from the Internet to no avail. As no action was taken, the brother then brought a claim in the domestic courts.

In January 2013, the district court ruled that there was no need to examine the request for the article to be removed from the Internet, as the applicant had de-indexed the article. It found, however, that the easy access via the Internet to information on the criminal proceedings from March 2008 to May 2011, when the applicant had de-indexed the article, had breached the claimants' right to respect for their reputation. It noted in particular that the applicant's failure to deindex the tags to the article meant that anyone could access the sensitive data on the proceedings by simply inserting the plaintiffs' names in the search engine. The applicant was order to pay €5,000 to each claimant in compensation. The Supreme Court upheld the first-instance decision on all grounds in June 2016.

2. Decision of the Court

The applicant complained under Article 10 of the Convention (freedom of expression) that there had been a breach of his right to impart information and that the €5,000 he had been ordered to pay in compensation to each claimant had been excessive.

Article 10

The Court noted that there was no dispute between the parties whether the applicant's freedom of expression, as guaranteed under Article 10 of the Convention, was interfered with by the domestic courts' decisions. Neither was it in dispute between the parties that such interference was "prescribed by law." Furthermore, the Court was satisfied that the interference in question was intended to protect "the reputation or rights of others" and thus pursued a legitimate aim under Article 10 § 2 of the Convention.

Regarding the question of whether the interference was necessary in a democratic society, the Court drew attention at the outset to the specificity and scope of the case at issue. The applicant was held liable not for failing to remove the article, but for failing to de-index it. De-indexing was defined as the activity of a search engine consisting of removing, on the initiative of its operators, from the list of results displayed following a search made on the basis of a person's name, internet pages published by third parties that contain information relating to that person. In the present case, the failure had allowed for the possibility, for a period whose length had been deemed by the domestic courts to be excessive, of typing into the search engine the claimants' names in order to access information relating to the criminal proceedings.

The Court viewed this as an important starting point from which to define the interference with the applicant's freedom of expression and to identify, accordingly, the applicable principles in order to assess the proportionality of that interference. Referring to older case law, the Court laid down relevant principles to guide its assessment and identified a number of criteria in the context of balancing freedom of expression against the right to reputation[264]. These criteria were the following: (i) contribution to a debate of general interest; (ii) the extent to which the person concerned is well known and the subject of the report in question; (iii)

[264] *Axel Springer AG v. Germany*, Grand Chamber judgment of 7 February 2012, no. 39954/08

the prior conduct of the person concerned towards the media; (iv) the method of obtaining the information in question, and its veracity; (v) the content, form and consequences of the publication in question; and (vi) the severity of the sanction imposed on the applicant.

There were several factual differences between the current case and older case law, and the Court ultimately acknowledged that the strict application of the criteria set out above would be inappropriate in the present circumstances. What must be considered was whether, in the light of the fundamental principles established in its case law, the domestic court's finding of civil liability on the part of the applicant was based on relevant and sufficient grounds, given the particular circumstances of the case. Special attention should be paid in this case to (i) the length of time for which the article was kept online; (ii) the sensitiveness of the data at issue; and (iii) the gravity of the sanction imposed on the applicant.

Regarding the first point, the Court acknowledged that the criminal proceedings were still pending at the time that the Supreme Court adopted its judgment in the applicant's case. However, it should be noted that the information contained in the article had not been updated since the occurrence of the events in question. Moreover, notwithstanding the formal notice sent to the applicant requesting the removal of the article from the Internet, it remained online and was easily accessible for eight months. Because of this, the applicable domestic law supported the idea that the relevance of the applicant's right to disseminate information decreased over the passage of time compared to the subject of the article's right to respect of their reputation, therefore shifting the balance in favour of the claimants.

With regard to the sensitivity of the data in question in the present case, the Court was mindful that the subject matter of the article was related to criminal proceedings. The circumstances in which information concerning sensitive data is published constituted a factor to be taken into account when balancing the right to disseminate information against the right of a data subject to respect for his or her private life.

Concerning the gravity of the sanction, the applicant was held liable under civil and not criminal law. Although the amount of compensation that the applicant was ordered to pay to the claimants for the breach of their right to have their reputations respected was not negligible, the Court was of the view that the severity of the sentence and the amount of compensation awarded in respect of

non-pecuniary damage (€5,000 to each claimant) was not regarded as excessive, given the circumstances of the case.

Where the balancing exercise between, on the one hand, freedom of expression protected by Article 10, and, on the other, the right to respect for one's private life, as enshrined in Article 8 of the Convention, had been carried out by the national authorities in conformity with the criteria laid down in the Court's case law, the Court was reluctant to substitute its view for that of the domestic courts.

The foregoing considerations were sufficient to conclude that the finding by the domestic courts that the applicant had breached the claimants' right to respect for his reputation by virtue of the continued presence on the Internet of the impugned article and by his failure to de-index it constituted a justifiable restriction of his freedom of expression. All the more so as no requirement was imposed on the applicant to remove the article from the Internet permanently.

Accordingly, there had been no violation of Article 10 of the Convention.

The interception and examination of communications by the UK Government was held to be in violation of Articles 8 and 10 despite a wide margin of appreciation given to the authorities on national security grounds

GRAND CHAMBER JUDGMENT IN THE CASE OF

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM

(Application no. 58170/13, 62322/14 and 24960/15)

25 May 2021

1. Principal Facts

The applicants in the first of these three joined cases were Big Brother Watch, English PEN, Open Rights Group and Dr Constance Kurz. The applicants in the second of the joined cases were the Bureau of Investigative Journalism and Alice Ross. The applicants in the third of the joined cases were Amnesty International, Bytes for All, Liberty, Privacy International, The American Civil Liberties Union, The Canadian Civil Liberties Association, The Egyptian Initiative for Personal Rights, The Hungarian Civil Liberties Union, The Irish Council for Civil Liberties, and the Legal Resource Centre.

The three applications were made in response to the revelations by Edward Snowden relating to the widespread use of electronic surveillance by the United States of America (USA) and the United Kingdom (UK). The applicants all believed that their electronic communications were likely to have been intercepted and/or accessed by the UK from communication service providers (CSPs). CPSs operate international sub-marine fibre optic cables that carry internet communication. Each cable may carry several "bearers", which transmit communication that has been divided into "packets" of data.

The surveillance schemes in question were run by the UK's Government Communication Headquarters (GCHQ) and the US's National Security Agency (NSA). GCHQ ran TEMPORA, which tapped into, and stored volumes of data drawn down from bearers. GCHQ collected communications that matched specific identifiers, such as an email address relating to a particular intelligence target. The collected communications were then opened and read by a GCHQ analyst only if they were considered to hold the highest value of intelligence. GCHQ also had a secondary processing system which automatically sorted a

small subset of collected communications against complex criteria. Matching material could then be potentially opened by analysts.

The legal framework for GCHQ electronic interceptions was contained in the Regulation of Investigatory Powers Act 2000 (RIPA), which allowed the Secretary of State to issue warrants for the interception of external electronic communications. RIPA did not allow the intercepted material to be read, looked at or listened to if the individuals involved were at that time in the British Islands.

The NSA ran two schemes, PRISM and Upstream. PRISM targeted specific material from Internet Service Providers (ISPs) and was regulated under the Foreign Intelligence Service Act (FISA), which required that applications for access to material gathered through PRISM be approved by the FISA Court of eleven senior judges. Upstream allowed the mass collection of content and communications from communication infrastructure owned by US communication service providers. This programme enabled the collection, storage and search of global data, in particular that of non-US citizens. Documents leaked by Edward Snowden suggest that GCHQ had access to PRISM from 2010.

RIPA specifically excluded the jurisdiction of the UK High Court in respect of human rights allegations against the intelligence services. Complaints were instead heard before the Investigatory Powers Tribunal (IPT) which was established to hear allegations by citizens of wrongful interference with their communications. The applicants in the first and second of the joined cases did not bring their complaints before the IPT while the applicants in the third of the joined cases lodged a complaint in 2013. The IPT hearing took place with both public and closed hearings, from the latter of which the IPT released previously secret information concerning the information sharing relationship between the UK and US intelligence services.

The IPT stated that the intelligence sharing regime with the NSA did not violate the Convention as it was in accordance with the law, its regulatory framework was effective, and it was subject to oversight and investigation by Parliament, an independent commissioner, and the IPT itself. The IPT ruled that the arrangements were accessible to the public with sufficient clarity and gave individuals adequate protection against arbitrary interference. The legal framework for the bulk interception of external (outside the UK) communications under section 8(4) RIPA, was also compatible with the Convention as it was in accordance with the law and there were safeguards in place to prevent security

analysts from examining the communications of people in the UK. Any indirect discrimination against individuals based on their national origin had been justified by national security considerations. In two individual instances the IPT found that the security services had breached their own rules and violated the Convention, the first due to a technical error and the second without any material loss to the claimant. Neither victim was awarded compensation.

2. Decision of the Court

The applicants complained about the Article 8 (right to respect for private and family life) and Article 10 (freedom of expression) compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA); the regime for the receipt of intelligence from foreign intelligence services; and the regime for the acquisition of communications data from communications service providers (CSPs).

On 13 September 2018 a Chamber of the Court handed down its judgment in the case. It was referred to the Grand Chamber under Article 43 at the request of the applicants.

The Bulk Interception of Communications (Section 8(4) Regime)

Article 8

The applicants complained that the regime for the bulk interception of communications (section 8(4) regime of RIPA) was incompatible with Article 8 of the Convention.

The Court began by noting the special difficulties in assessing the regime. Bulk surveillance is not targeted at individuals and therefore has the capacity to have a very wide reach, both inside and outside the territory of the surveilling State. While safeguards are pivotal, they are elusive in practice, considering that they are predominately used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. Due to this, Contracting States have a legitimate need for secrecy, which will mean little, if any, information is known about the operation of such schemes. Furthermore, the threats facing Contracting States have proliferated, including global terrorism, human trafficking, and the sexual exploitation of children. Many of these threats operate

via international networks of hostile actors, with access to technology that can disrupt digital infrastructure, cause cyber-attacks and threaten national security. Consequently, the Court recognised the valuable capacity of bulk interception regimes to identify new threats in the digital domain and sought to assess such regimes for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse.

The Court viewed the bulk interception of communication as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses. The stages of the bulk interception process could be described as:

(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);
(b) the application of specific selectors to the retained communications/related communications data;
(c) the examination of selected communications/ related communications data by analysts; and
(d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties.

Each four stages were found to interfere with an individuals' Article 8 rights. Although the initial interception does not constitute a significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. At the final stage, where information about a person is analysed or the contents of the communication is examined by an analyst, the need for safeguards will be at its highest. Thus, when examining whether the interference is justified, the Court based its assessment of the section 8(4) regime on the basis of this progressive interference.

On whether the inference was justified, the Court noted the general principles established in earlier case law, which affirmed that bulk interception regimes did not per se fall outside the State's margin of appreciation. In view of the proliferation of threats that States currently face from networks of international actors using sophisticated technology, the Court considered that the decision to operate a bulk interception regime in order to identify threats to national security or against essential national interests fell within the State's margin.

The Court then sought to determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such an assessment should focus on whether the domestic legal framework contained sufficient guarantees against abuse and whether the process was subject to "end-to-end safeguards". In doing so, the assessment should have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse.

In assessing whether the State has acted within its margin of appreciation, the Court was satisfied that the section 8(4) Regime pursued the legitimate aims of protecting national security, preventing disorder and crime and protecting the rights and freedoms of others. The Court also accepted that the domestic law was adequately accessible, considering that the legislative provisions governing the operation of the bulk interception regime were elucidated in the Interception of Communications Code of Practice ("the IC Code"). The IC Code was a public document that provided details of how the regime operated in practice.

The Court next turned to whether the law contained adequate and effective safeguards and guarantees to meet the requirements of "foreseeability" and "necessity in a democratic society". Here, the Court built on previous case law and established criteria to assess the interception of the contents of communications, namely, whether the domestic legal framework clearly defined:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent ex post facto review of

such compliance and the powers vested in the competent body in addressing instances of non-compliance.

On analysis of each criterion, the Court ultimately held that the section 8(4) regime, despite its safeguards, including some robust ones, did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. Inherent in the bulk interception regime was the potential for it to be abused in a manner adversely affecting the rights of individuals to respect for private life. In particular, the Court identified fundamental deficiencies in the regime, such as, inter alia, the failure to include the categories of selectors in the application for an interception warrant and the failure to subject selectors linked to an individual to prior internal authorisation. While the IC Commissioner provided independent and effective oversight of the regime, and the IPT offered a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services, these important safeguards were not sufficient to counterbalance the shortcomings.

In view of the above, the Court found that that the section 8(4) regime did not meet the "quality of law" requirement of Article 8 and was therefore incapable of keeping the "interference" to what was "necessary in a democratic society". Accordingly, there was a violation of Article 8.

Article 10

Under Article 10, the Court considered whether the section 8(4) regime violated the protection afforded to journalists, namely the protection of privileged communications.

The Court affirmed that the safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of the freedom of the press. An interference with the protection of journalistic sources cannot be compatible with Article 10 unless it is justified by an overriding requirement in the public interest. Any interference with the right to protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake.

The Court accepted that the section 8(4) regime interfered with journalists' rights under Article 10 to freedom of expression. The regime had a clear basis in

law, however, in assessing foreseeability and necessity under Article 8, the Court already identified deficiencies in the regime and safeguards, such as the absence of prior internal authorisation for selectors linked to an identifiable individual.

In the context of Article 10, the Court reviewed existing safeguards in respect of confidential journalistic material set out in the IC Code and found them adequate for the purposes of Article 10. However, the safeguards did not address the weaknesses identified by the Court in its analysis of the regime under Article 8 and did not satisfy the requirements of legal procedural safeguards under Article 10. In particular, there was no requirement that the use of selectors or search terms known to be connected to a journalist be authorised by a judge or other independent decision-making body vested with the power to determine whether it was "justified by an overriding requirement in the public interest" and whether a less intrusive measure might have sufficed to serve the overriding public interest. Moreover, the IC Code only required "particular consideration" be had of an interception that may have contained confidential journalist material, as opposed to requiring a judge or independent body to rule on its continued storage.

In view of the identified weaknesses, the Court found that there had also been a breach of Article 10 of the Convention by virtue of the operation of the section 8(4) regime.

The Receipt of Intelligence from Foreign Intelligence Services

Article 8

The applicants complained about the receipt by the UK authorities of material from foreign intelligence services. Specifically, that the respondent State's receipt of material intercepted by the NSA under PRISM and Upstream was in breach of their rights under Article 8 of the Convention.

The Court reaffirmed the scope of the Contracting State's responsibility under Article 8 as the initial request and the subsequent receipt of intercepted material, followed by its subsequent storage, examination and use by the intelligence services of the receiving State. In addition, where a request was made to a non-contracting State for intercept material, the request must have a basis in domestic law and that law must be accessible to the person concerned and foreseeable as to its effects. Furthermore, any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or

to directly access such material, should be subject to independent supervision, and the possibility for independent ex post facto review.

The Court considered that the regime for requesting and receiving intelligence from non-Contracting States had a clear basis in domestic law and was adequately accessible. The regime undoubtedly pursued the legitimate aims of protecting national security, preventing disorder and crime and protecting the rights and freedoms of others.

In regard to the foreseeability and necessity of the regime, the Court considered that there were clear detailed rules which gave citizens an adequate indication of the circumstances in which the authorities were empowered to make a request to a foreign intelligence service. In addition, the Court was satisfied that the UK had in place adequate safeguards for the examination, use, storage, onward transmission, erasure and destruction of the material. A further layer of protection was also granted by the IC Commissioner and the IPT, which provided oversight of the intelligence sharing regime and ex post facto review respectively.

Due to the above findings, the Court was of the opinion that the regime for requesting and receiving intercept material was compatible with Article 8 and accordingly found no violations.

Article 10

The applicants complained that the intelligence sharing regime had breached their rights under Article 10. However, the Court found that the complaint gave rise to no separate issue over and above that rising out of Article 8. Therefore, there had also been no violation of Article 10.

Acquisition of Communications Data from Communications Service Providers

Article 8

The applicants complained that the regime for the acquisition of communications data under Chapter II of RIPA was incompatible with their rights under Article 8.

The Chamber had previously held that domestic law required that any regime permitting the authorities to access data retained by CSPs should limit access to

the purpose of combating "serious crime", and that access should be subject to prior review by a court or independent administrative body. Since the current regime did not meet this requirement, the Chamber held that it could not be "in accordance with the law" within the meaning of Article 8.

The Government did not contest the Chamber's findings, and the Grand Chamber found no ground on which to disagree with the Chamber's conclusions. Accordingly, there had been a violation of Article 8.

Article 10

The applicants complained under Article 10 about the regime for the acquisition of communications data from CSPs.

The Chamber had previously acknowledged that the Chapter II regime afforded enhanced protection where data were sought for the purpose of identifying a journalist's source. However, these protections only applied where the purpose was to determine a source and did not apply in every case where there was a request for the communications data of a journalist, or where such collateral intrusion was likely. Consequently, the Chamber considered that the regime was not "in accordance with the law" for the purpose of the Article 10.

The Government did not contest the Chamber's findings, and the Grand Chamber found no ground on which to disagree with the Chamber's conclusions. Accordingly, there had been a violation of Article 10.

Article 41

The Court awarded to the applicants in the first of the joined cases €227,500; to the applicants in the second of the joined cases €90,000; and to the applicants in the third of the joined cases €36,000 in costs and expenses. The applicants did not submit any claim in respect of pecuniary damages and so the Court did not award any.

Complaint regarding the anonymisation of court documents in an online database and a rule deferring the publication of judicial decisions declared inadmissible, as Article 10 could not apply to abstract information which was not instrumental for the exercise of the applicants' right to freedom of expression

DECISION IN THE CASE OF

BORIS ANTONOV MITOV AND OTHERS v. BULGARIA

(Application no. 80857/17)

28 February 2023

1. Principal facts

The applicants were eight Bulgarian journalists from various media outlets who specialised in reporting on matters relating to the judiciary. In October 2016, the applicants sought judicial review of the internal anonymisation rules which had been recently laid down by the President of the Supreme Administrative Court ("the SAC") following proceedings before the Commission for Personal Data Protection after a complaint from two individuals that the SAC had unlawfully processed their personal data. The Commission had fined the SAC, and instructed it to bring all documents published in its online database containing personal data of individuals in line with the requirements of the personal data protection legislation. The rules therefore provided for the redaction of personal data in all documents published in the SAC's online database.

The applicants had sought judicial review against Rules 1, 2 and 3. Rule 1 provided the type of documents that the database would contain, with any personal data to be redacted from all of them. Rule 2 set out thirteen categories of "personal data" that would be redacted from those documents, and Rule 3 stated that since scanned case material could not be redacted in that manner, it would not be made available online. The applicants were particularly concerned that the rules did not provide for the online publication of administrative decisions under challenge or claims for judicial review. The applicants further complained that the categories of data subject to redaction under Rule 2 were not personal data, or had been defined too broadly to be personal data in all cases. In February 2017 the Sofia City Administrative Court declared the two claims lodged by the applicants inadmissible. Although the applicants appealed against this decision, in May 2018 the SAC upheld the lower court's decision.

In November 2017, an amendment to Section 64(1) of the Judiciary Act 2007 came into force (the "deferred publication rule"). Section 64(1) had originally introduced the requirement for all judicial decisions to be published on the relevant court's website, although this had been amended in 2009 to provide that these decisions would be published online immediately after being delivered. Under the deferred publication rule, judicial decisions in criminal cases which convicted and sentenced someone or which upheld convictions and sentences would only be published online after the prosecuting authorities had informed the relevant court that steps had been taken to enforce them.

2. Decision of the Court

The applicants complained under Article 10 of the Convention about the anonymisation rules laid down by the President of the SAC in September 2016, and about the November 2017 legislative amendment bringing into force the deferred publication rule.

Admissibility of the complaint about the SAC's 2016 anonymisation rules

Article 10 does not bestow an unfettered, automatic right to access information held by the authorities, nor does it oblige the authorities to impart such information on request. Emphasising that Article 10 rights are engaged only if access to such information is critical for the exercise of the right to freedom of expression, the Court underscored that in the present case, none of the case-law criteria for determining that threshold had been met. These criteria were; (a) the purpose of the information request; (b) the nature of the information sought; (c) the particular role of the seeker of the information in "receiving and imparting" it to the public; and (d) whether the information is ready and available.

In accordance with settled case-law principles, the above criteria were to be assessed in the light of the particular circumstances of each case. In the present case, the applicants' complaint did not concern a specific piece of information, or a defined category of information held by a public authority, but was rather founded on the purely abstract issue of the impossibility of accessing all the scanned case material available in the database of the SAC. Settled case-law held that an applicant could not complain of a restriction on access to information in the abstract, and had also held that general statements on why certain types of information held by the authorities ought to be made available were not sufficient to engage Article 10. As there was no exact specific information

which the applicants were complaining about being unable to access, it could not be said that being granted such access was instrumental for the exercise of their right to freedom of expression. Article 10 therefore could not and did not apply, as there were no particular circumstances on the basis of which to apply the threshold criteria. Hence, the complaint was rejected as being incompatible ratione materiae with the provisions of the Convention.

Admissibility of the complaint about the deferred publication rule for certain criminal judgments

The Government argued that the applicants could not be victims as they had not referred to any specific case in which the deferred publication rule had hindered their work, but were merely complaining about the rule itself. As there was no evidence that the deferred publication rule had prevented the applicants from accessing specific information, the rule could not in itself have affected their right to freedom of expression. As with the finding under the SAC's anonymisation rules, the Court reiterated its position that Article 10 could not be engaged as it could not be determined that the information to which the applicants sought access to was crucial for the exercise of their right to freedom of expression.

The Court therefore found that Article 10 did not apply, and the complaint was rejected as being incompatible *ratione materiae* with the provisions of the Convention. The application was therefore declared inadmissible and dismissed.

The police's interception of the applicant's communications, the lack of adequate safeguards and consequently increased risk of arbitrariness was inconsistent with the requirement of lawfulness, which constituted a violation of Article 8

GRAND CHAMBER JUDGMENT IN THE CASE OF
BYKOV v. RUSSIA

(Application no. 4378/02)
10 March 2009

1. Principal facts

The applicant was a Russian national who was born in 1960 and lived in Russia. At the time of his arrest in October 2000 he was a major shareholder and an executive of a corporation, and also a member of the Krasnoyarsk Regional Parliamentary Assembly.

In September 2000 the applicant allegedly ordered V., a member of his entourage, to kill Mr S., a former business associate. V. did not comply with the order, but he reported the applicant to the Federal Security Service ("the FSB"). The FSB and the police decided to conduct a covert operation to obtain evidence of the applicant's intention to murder S. On 29 September 2000 the police staged the discovery of two dead bodies at S.'s home. They officially announced in the media that one of those killed had been identified as S. The other man was his business partner, Mr I.

On 3 October 2000 V. went to see the applicant at his home. He carried a hidden radio-transmitting device while a police officer outside received and recorded the transmission. Following the instructions he had been given, V. engaged the applicant in conversation, telling him that he had carried out the murder. As proof he handed the applicant several objects borrowed from S. and I. The police obtained a 16-minute recording of the conversation between V. and the applicant. On 4 October 2000 the applicant's house was searched. The objects V. had given him were seized. The applicant was arrested and remanded in custody. He was charged with conspiracy to commit murder and conspiracy to acquire, possess and handle firearms.

The applicant's pre-trial detention was extended several times and his numerous appeals and requests for release were rejected because of the gravity

of the charges against him and the risk that he might abscond and bring pressure to bear on the witnesses. In June 2002 the applicant was found guilty on both counts and sentenced to six and a half years' imprisonment. He was conditionally released on five years' probation. The sentence was upheld on appeal.

2. Decision of the Court

The applicant complained under Article 5 § 3 that his pre-trial detention had been excessively long and that it had been successively extended without any indication of relevant and sufficient reasons. Under Article 6 § 1, he complained that the proceedings against him had been unfair, as the police had set a trap to trick him into incriminating himself in his conversation with V. and the court had admitted the recording of the conversation in evidence at the trial. The applicant also complained that the covert operation by the police had involved an unlawful intrusion into his home and that the interception and recording of his conversation with Mr V. amounted to an interference with his private life and his correspondence, in breach of Article 8.

Article 5 § 3

The continued pre-trial detention could be justified only if there were specific indications of a genuine public-interest requirement which, notwithstanding the presumption of innocence, outweighed the rule of respect for individual liberty laid down in Article 5 of the Convention. The Court found, however, that grounds for detention in this case had not been at all substantiated by the courts concerned, particularly during the initial stages of the proceedings, and that there had therefore been a violation of Article 5 § 3.

Article 6 § 1

The Court reiterated that Article 6 guaranteed the right to a fair trial as a whole, and did not lay down any rules on the admissibility of evidence as such, even evidence obtained unlawfully in terms of domestic law. In that connection it observed that the applicant had been able to challenge the methods employed by the police, in the adversarial procedure at first instance, and on appeal. He had thus been able to argue that the evidence adduced against him had been obtained unlawfully and that the disputed recording had been misinterpreted. The domestic courts had addressed all these arguments in detail and had dismissed each of them in reasoned decisions. The Court further noted that the statements

by the applicant that had been secretly recorded had not been made under any form of duress; had not been directly taken into account by the domestic courts, which had relied more on the expert report drawn up on the recording; and had been corroborated by a body of physical evidence. The Court thus concluded that the applicant's defence rights and his right not to incriminate himself had been respected, and that accordingly there had been no violation of Article 6 § 1.

Article 8

The Court observed that it was not disputed that the measures carried out by the police had amounted to an interference with the applicant's right to respect for his private life. It pointed out that for such an interference to be compatible with the Convention, it had to be in accordance with the law, and necessary in a democratic society for one of the purposes listed under Article 8 § 2.

The Court noted that the Russian Operational-Search Activities Act was expressly intended to protect individual privacy by requiring judicial authorisation for any operational activities that might interfere with the privacy of the home or the privacy of communications by wire or mail services. In the applicant's case, the domestic courts had held that since V. had been invited to the applicant's home and no wire or mail services had been involved (as the conversation had been recorded by a remote radio-transmitting device), the police operation had not breached the regulations in force.

In that connection, the Court reiterated that in order for the lawfulness requirement in Article 8 to be satisfied with regard to the interception of communications for the purpose of a police investigation, the domestic law must provide protection against arbitrary interference with an individual's right under Article 8, and had to give a sufficiently clear indication as to the circumstances in, and the conditions on which the police authorities were empowered to resort to such measures. Furthermore, the Court emphasised that the law must indicate the scope of any such discretion conferred on the competent authorities, and the manner of its exercise. In the present case, the Court considered that the use of a remote radio-transmitting device to record the conversation between V. and the applicant was virtually identical to telephone tapping, in terms of the nature and degree of the intrusion into the privacy of the individual concerned. It considered that the applicant had not benefited from what amounted to a negligible safeguarding procedure by which his conversation with V. had been intercepted, and that the scope and manner of the authorities' ability to exercise

its discretion had not been defined. The Government's argument that the necessary requirements were met by the possibility for the applicant to bring court proceedings against the legality of the "operative experiment" did not satisfy the Court, especially given the absence of specific safeguarding regulations. Finally, it noted that since the law regulated only the interception of communications by wire and mail services, the legal discretion enjoyed by the police authorities in employing the surveillance technique had been too broad, and was accordingly open to arbitrariness and failed to meet the lawfulness requirement, the Court considered that the interference with the applicant's right to respect of private life was not in accordance with the law. The Court was therefore not required the determine whether the interference was necessary in a democratic society, nor whether there had been an interference with the applicant's right to respect for his home, Hence, there had been a violation of Article 8.

Article 41

The Court awarded the applicant €1,000 in respect of non-pecuniary damage and €25,000 for costs and expenses.

The Swedish Government's failure to ensure sufficient safeguarding procedures to prevent the risk of abuse of its bulk-interception information surveillance regime led to the finding of a violation of Article 8

GRAND CHAMBER JUDGMENT IN THE CASE OF

CENTRUM FÖR RÄTTVISA v. SWEDEN

(Application no. 35252/08)

25 May 2021

1. Principal facts

The applicant, Centrum för rättvisa, was a Swedish not-for-profit organisation that represented clients in proceedings concerning rights and freedoms under the Convention or related proceedings under Swedish law. The applicant believed that due to the nature of its function as an non-governmental organisation scrutinising the activities of State actors, there was a risk that its communications through mobile telephones and mobile broadband had been or would be intercepted and examined by way of signals intelligence.

The applicant contested specific legislation on signals intelligence, the Signals Intelligence Act ("the SIA"), which authorised the National Defence Radio Establishment (Försvarets radioanstalt, "the FRA") to conduct signals intelligence, which established a system of secret surveillance which potentially affected all users of mobile phone services and the internet without any notification to users about such surveillance. As there was no domestic remedy which provided any grounds of appeal for an individual who suspected that they had had their communications intercepted, the applicant argued that the SIA amounted to an interference with its rights under Article 8.

2. Decision of the Court

The applicant complained that the Swedish legislation and practice in the field of signals intelligence, specifically regarding the bulk-interception of communications, violated its right to respect for private life and correspondence under Article 8 of the Convention, and that it did not have an effective remedy contrary to Article 13.

On 19 June 2018, a Chamber held that there had been no violation of Article 8 and that there was no need to examine separately the complaint under Article 13. The case was referred to the Grand Chamber in accordance with Article 43 at the request of the applicant.

Admissibility

The Government first objected to the applicant's victim status, arguing that they did not belong to a "group of persons or entities targeted by the legislation" on signals intelligence within foreign intelligence. The Government also argued that the SIA did not directly affect all users of mobile telephone services and the internet as it was restricted to foreign intelligence, and that as the applicant's telephone and internet communications were unlikely to be intercepted, there was a virtually non-existent risk that they would be retained for further scrutiny beyond the automatic processing stage. As there would be no interference with Article 8 rights until the stage when an analytical examination of selected signals was possible, the Government therefore requested that the Grand Chamber declare the application inadmissible for lack of victim status.

The Court noted that an applicant may claim to be the victim of a violation of their Convention rights by the mere existence of legislation permitting secret surveillance measures. The two primary established criteria for victimhood were firstly examining whether the scope of the legislation "directly affects all users of communication services by instituting a system where any person can have his communications intercepted", and secondly, by taking into account "the availability [and effectiveness] of remedies at the national level". Noting that the applicant had not claimed to belong to a group of persons specifically targeted by the legislation, the Court rejected the Government's argument against the applicant's victim status, and agreed with the applicant that the SIA facilitated the possibility that the communications of any person or entity in Sweden may be subject to at least the initial stages of automatic processing by the FRA. As the domestic remedies available in Sweden were subject to certain limitations, with the practical result that the mere threat of surveillance under the Swedish bulk interception legislation could itself be found to restrict free communication, it was found that this could constitute, for all users or potential users, a direct interference with their Article 8 rights. It was accordingly determined that the applicant had victim status, the application was declared admissible.

Article 8

Turning first to the existence of an interference, the Court outlined four general stages of the bulk-interception process, and stated that it viewed bulk-interception as a gradual process whereby the degree of interference with individuals' Article 8 rights increased as the process progressed. Article 8 applied at each of the four stages, but at the end of the process, where information about a particular person or the content of the communications is examined by an analyst, the need for safeguards against abuse would be at its highest. The existence of an interference of the applicant's Article 8 rights was therefore established and confirmed by the Court in the present case.

It was then considered whether the interference was justified, and the Court reiterated the settled case-law principles that such an interference could only be justified if it was in accordance with the law, pursued one or more of the legitimate aims, and was necessary in a democratic society. It was uncontested between the parties both that the interference was in accordance with the law, and that it pursued the legitimate aim of protecting national security.

It was highlighted that States enjoy a wide margin of appreciation to decide which type of interception regime would be necessary to achieve the legitimate aim of protecting national security. Due to the development of technology in the field of security surveillance, it was necessary to re-evaluate the six minimum safeguarding requirements which had been developed in previous case-law specifically for targeted interceptions, to reflect the inherent risk of abuse and the legitimate need for secrecy under a bulk-interception regime. Therefore, in order to assess whether the respondent State acted within its margin of appreciation regarding its bulk-interception regime, the Court set out and examined a further eight requirements to determine whether the Swedish domestic legal framework provided sufficient guarantees against abuse, and whether the process was subject to the required "end-to-end safeguards".

Each of the eight requirements were addressed in turn to determine whether the law contained the adequate and effective safeguards and guarantees to met the criteria of "foreseeability" and "necessity in a democratic society", and the Court identified shortcomings with three of the eight requirements.

Under the fifth requirement, the precautions to be taken when communicating intercepted material to other parties, the Court identified a serious shortcoming in

the absence of an express legal requirement for the FRA to assess the necessity and proportionality of intelligence sharing when information seriously compromising Article 8 rights was present in material to be transmitted abroad. The signals intelligence legislation in force at the time could allow information which critically violated privacy rights to be transmitted abroad, even in circumstances where the transmission was not of any significant intelligence value.

Under the sixth requirement, the Court found a further shortcoming with the absence of any provision obliging the FRA to cancel an information interception mission if the conditions for it had ceased to exist or the measures themselves were no longer necessary. The applicant argued that this facilitated the possibility of excessive and inappropriate surveillance missions lasting for several months longer than would be necessary. However, it was found that there were sufficient mechanisms in place for the cancellation of a bulk interception mission to meet the safeguarding requirement, and similarly found only a minor procedural shortcoming with the absence of any provision on destroying intercepted material which did not contain personal data.

Under the eighth and final requirement for an independent ex post facto review, the Court found a further significant shortcoming in the safeguarding mechanism that the SIA provided for an ex post facto review on the initiative of individuals or legal persons without the need for them to demonstrate that they may have been affected by a bulk interception operation. Under the mechanism, the Foreign Intelligence Inspectorate must investigate if the individual or legal person's communications have been intercepted, and then verify whether the interception was in accordance with the law. It was found that as the Inspectorate also had a duty to supervise and monitor the FRA's activities, this dual role could lead to situations where the Inspectorate would have to assess its own activities in supervising bulk interception by the FRA, leading to a clear possibility of a conflict of interest. In combination with the lack of an avenue for members of the public to obtain reasoned decisions in response to complaints regarding bulk interception of communications, the Court held that the ex post facto review system was not an effective safeguard.

Taking into account its examination of the shortcomings found under several of the Court's domestic law safeguarding requirements, the Court held that there had been a violation of Article 8 due to the respondent State's failure to comprehensively meet the requirement of "end-to-end" safeguards. As the highlighted shortcomings were not sufficiently compensated for by the existing

safeguards, the Swedish bulk-interception regime overstepped the margin of appreciation given to States and did not meet the threshold for adequate and effective guarantees against arbitrariness and the risk of abuse.

Article 13

The Chamber had found that no separate issue arose under Article 13, the Grand Chamber adopted the same conclusion, with regard to its finding that there had been a violation of Article 8.

Article 41

The applicant had stated that a finding of a violation would constitute sufficient redress, and the Court accordingly made no award under this head. The Court awarded €52,625 to the applicant for costs and expenses.

The reading out at trial of transcripts of telephone conversations intercepted in the context of criminal proceedings and their release into the public domain violated Article 8

JUDGMENT IN THE CASE OF
CRAXI v. ITALY (No. 2)

(Application no. 25337/94)
17 July 2003

1. Principal facts

The applicant was born in 1934. He was General Secretary of the Italian Socialist Party from 1976 to 1993 and Prime Minister of Italy from 1983 to 1987. From 1994 he lived in Tunisia, and when he passed away in 2000 his family continued the proceedings. During the so called "clean hands" campaign in Italy, the applicant in 1994 was charged with corruption, dishonest receipt of money, concealment of dishonest gain and illegal financing of political parties.

The public prosecutor obtained an order from the District Court for the applicant's telephone calls between Italy and his home to be intercepted. At the hearing of the criminal proceedings, the public prosecutor filed the transcripts of the intercepted telephone calls with the court registry and asked that they be admitted as evidence. The prosecution also read out several extracts in court, and the contents of certain conversations and the names of the people speaking were subsequently published in the press.

2. Decision of the Court

The applicant complained that the release into the public domain of intercepted telephone conversations of a private nature, and in particular the prosecutor's decision to deposit the transcripts in the court registry, violated his rights under Articles 8, 14 and 18 of the Convention.

Article 8

The Court reiterated that telephone conversations are covered by the notions of "private life" and "correspondence" within Article 8. The reading out at the hearing and the disclosure of the content of the telephone interceptions to the

press therefore amounted to interferences with Article 8. It was thus necessary to consider whether the interferences were in accordance with the law and proportionate to a legitimate aim.

In respect of the publication by the press of passages of the telephone conversations, the Court recalled the importance of freedom of expression in a democratic society. The press reporting, including commenting, on court proceedings contributes to their publicity and is in accordance with the requirement under Article 6 § 1 that hearings be public. The media have the task of imparting information and ideas, and the public has a right to receive them, especially when a public figure is involved. However, the public interest in receiving information only covers facts which are connected with the criminal charges brought against the accused. The press should abstain from publishing information, which is likely to prejudice, whether intentionally or not, the Article 8 right of the accused persons.

In the present case, the Court observed that some of the conversations published in the press were of a strictly private nature; their content had little, or no connection, with the criminal charges. Their publication by the press did not meet a pressing social need. The interreference was therefore not proportionate to the legitimate aims which could have been pursued by the publication and consequently not necessary in a democratic society.

In respect of whether the interference complained of could be imputed to the State, the Court noted that the publication was made by private newspapers, which were not under the control of the public authorities. The source of the journalists' information was also not the reading out of the conversations during the hearing, but the bulk of the interceptions deposited in the court registry. The Court did not accept that by depositing the interceptions in the registry, the public prosecutor had chosen to release them into the public domain, since under domestic law the deposit of a document only rendered it accessible to the parties. The Court therefore concluded that the divulging of the conversations to the press was likely to have been caused either by a malfunction of the registry or by the press obtaining the information from one of the parties to the proceedings, or from their lawyers.

However, the Court reiterated the positive obligation under Article 8 on a State to take the necessary steps to ensure effective protection of an individual's right to respect for his private life and correspondence. This will include making available appropriate safeguards to prevent a disclosure of a private nature, and

carrying out an effective inquiry to rectify the matter to the extent possible when such a disclosure has taken place. In the present case, the Court concluded that the domestic authorities had failed in these obligations. The authorities had failed to provide safe custody of the transcripts and it did not appear that an effective inquiry had been carried out. The Court therefore held that the State had not fulfilled its obligations to secure the applicant's right to respect for his private life and correspondence, and there had thus been a violation of Article 8.

In respect of the reading out at trial of the content of some of the interceptions of the telephone conversation, the Court first considered whether the interference was "in accordance with the law". The Court reiterated that it is primarily for the national authorities to interpret and apply the relevant internal rules, though the Court can and should exercise a certain power to review whether domestic law has been complied with.

In the present case, under the Code of Criminal Procedure ("CCP"), after the public prosecutor filed the transcripts of the intercepted conversation with the court registry, there should have been a hearing in private to determine which material should be excluded. The aim of these procedural requirements was to provide the parties and the judge with an opportunity to select the interceptions which were of no relevance and whose disclosure could have adversely interfered with the accused's right to respect for private life and correspondence. If applied this would have constituted a substantial safeguard.

The District Court had held that these provisions of the CCP did not apply to the applicant's case, however nothing in the District Court's order explained why these guarantees could not be respected and the Court considered that the CCP should have applied. The Court therefore considered that the interference was not "in accordance with the law", as the applicant had been deprived of the substantial procedural safeguards provided by domestic law without proper explanations being given by the domestic tribunals. It was not necessary to consider whether the interference pursued a "legitimate aim" or was "necessary in a democratic society".

Articles 14 and 18

The Court noted that the complaints under Articles 14 and 18 arose out of the same facts as those examined in respect of Article 8. Given its decision on Article 8, it was not necessary for the Court to examine the case under Articles 14 and 18.

Article 41

The Court awarded the applicant's heirs a total of €6,000 in respect of non-pecuniary damage.

The failure to include relevant and specific details in the secret surveillance orders concerning a case of telephone tapping of a drug-trafficking suspect meant that adequate and sufficient safeguards against potential abuse were not met, which constituted a violation of Article 8

JUDGMENT IN THE CASE OF
DRAGOJEVIC v. CROATIA

(Application no. 68955/11)
15 January 2015

1. Principal facts

The applicant was a Croatian national, who worked as a sailor on for a shipping company headquartered in Croatia.

In 2007, the police and State Attorney's Office for the Suppression of Corruption and Organised Crime ('the OSCOC') investigated allegations of possible drug trafficking between Latin America and Europe via ocean carriers, involving several persons from Croatia. On the basis of a police report, in March 2007 the OSCOC requested and was granted authorisation to use secret surveillance measures to tape the applicant's telephone and covertly monitor him.

In January 2009, the applicant was arrested and detained on suspicion of drug trafficking. He was indicted in March 2009 on charges of drug trafficking and money laundering. His lawyer asked the Dubrovnik County Court for access to audio recordings obtained by the use of secret surveillance measures and the request was granted. The applicant then lodged an objection against the indictment on the basis that the results of the secret surveillance measures did not suggest that he had been involved in the offence. This objection was dismissed as ill-founded on the basis that there was insufficient suspicion to warrant sending the case for trial.

The applicant then applied to have the results of the secret surveillance measures excluded from the case file as unlawfully obtained evidence on the grounds that the orders for their use had not been sufficiently reasoned and had thus been unlawful under domestic law. The president of the trial bench dismissed the request as ill-founded. During this period, the applicant's pre-trial detention was extended numerous times.

In December 2009 the Dubrovnik County Court found the applicant guilty on charges of drug trafficking and money laundering and sentenced him to nine years' imprisonment. The judgment was based, among other things, on witness statements, evidence obtained through numerous searches and seizures and on the use of secret surveillance measures. His conviction was upheld by the Supreme Court in September 2010 and his constitutional complaint was dismissed in May 2011.

2. Decision of the Court

Relying on Article 8, the applicant complained about the secret surveillance of his telephone conversations. He also complained under Article 6 § 1 about the unfairness of the proceedings against him, alleging: a lack of impartiality of the trial; and unfairness due to the fact that his conviction had been based on evidence obtained by unlawful secret surveillance measures.

Article 8

The Court noted that it was not in dispute that covertly monitoring the applicant's telephone had constituted an interference with his rights under Article 8. The central question was whether the system of secret surveillance, as applied by the Croatian authorities, provided adequate safeguards against abuse.

Domestic law clearly provided for any secret surveillance measures in the context of criminal proceedings to be lawful, provided that they had been ordered by an investigating judge upon a request by the State Attorney. The Court considered that requiring the authorisation of secret surveillance to be in written form, and containing a statement of reasons, meant that domestic law provided for prior authorisation of the use of secret surveillance measures, which must be sufficiently thorough and capable of demonstrating that the statutory conditions for the use of secret surveillance had been met, and that use of such measures was necessary and proportionate in the given circumstances.

The Court emphasised that a detailed statement of reasons was necessary when ordering the use of secret surveillance measures, as this guaranteed the existence of a probable cause to believe that an offence proscribed under the law had been committed. The authority which approves the use of secret surveillance must confine it to cases in which there are factual grounds for suspecting a person of planning or committing a serious criminal act. Surveillance measures should

only be ordered if there is no prospect of successfully establishing the facts by another method, or where doing so would be considerably more difficult. This ensures that secret surveillance measures are not ordered arbitrarily, irregularly or without due and proper consideration.

In the applicant's case, the four secret surveillance orders issued by the investigating judge of the Zagreb County Court were essentially based on a statement referring to the existence of the OSCOC's request for the use of secret surveillance. No actual details were provided which referred to the specific facts of the applicant's case, nor was there any reference to the particular circumstances which indicated a probable cause to believe that the offences had been committed or that the investigation could not be conducted by other means.

Though the statutory requirements concerning prior judicial scrutiny and detailed reasons had not been complied with, the practice of the County Court had been approved by the Supreme Court. In doing so, the national courts had effectively introduced the possibility of retrospective justification, where the statutory requirements had not been complied with. The Court stated that a circumvention of this requirement by retrospective justification did not provide adequate and sufficient safeguards against potential abuse. Such a practice 'open[ed] the door to arbitrariness by allowing the implementation of secret surveillance contrary to the procedure envisaged by the relevant law.'

In considering the applicant's opportunity to challenge the lawfulness of the surveillance measures, the Court noted that the criminal courts had limited their assessment of the use of secret surveillance to the question of whether the evidence thus obtained was to be admitted, without going into the substance of his allegations of arbitrary interference with his Article 8 rights. Finally, the Croatian Government had not provided any information on remedies which would be available to a person in the applicant's situation.

Accordingly, there had been a violation of Article 8.

Article 6

The Court made clear that the mere fact that one of the judges sitting on the bench had also been involved in the decisions to extend the applicant's pre-trial detention did not raise an issue of lack of impartiality under the Convention.

In relation to the use of evidence obtained by secret surveillance, the Court observed that the applicant had not disputed the reliability of the information obtained by those measures, instead limiting his objection to the formal use of it as evidence during the proceedings. Since the applicant was given an opportunity to challenge the authenticity of the evidence, and it was not the only evidence upon which the conviction was based, the Court considered that there was nothing to substantiate the conclusion that his defence rights had not been properly complied with.

Accordingly, there had been no violation of Article 6 § 1.

Article 41

The Court held that Croatia was to pay the applicant €7,500 in respect of non-pecuniary damages and €2,160 in respect of costs and expenses.

An order by an investigating judge authorising the use of a suspect's personal telephone call data in a criminal investigation did not breach Article 8

JUDGMENT IN THE CASE OF
FIGUEIREDO TEIXEIRA v. ANDORRA

(Application no. 72384/14)
8 November 2016

1. Principal facts

The applicant was born in 1983 and lived in Andorra.

The applicant was arrested on 5 December 2011 in relation to suspected drug trafficking. The judge responsible for the criminal investigation (the 'batlle') in an order dated 30 August 2012 asked a telephone company (Andorra Telecom) to provide (a) a list of incoming and outgoing calls from two telephone numbers belonging to the applicant from 15 August 2011 to 4 December 2011; and (b) the identities of subscribers holding the numbers in that list (together referred to as the "impugned measure").

The applicant sought to set aside the batlle's order on the basis that it breached his right to the secrecy of his communications. The battle's dismissed this application and the applicant's appeals were also dismissed. The Constitutional Court also dismissed the applicant's appeal, having found that the storage of customers' data was provided for under Andorra Telecom's general terms and conditions of sale. Andorra's Code of Criminal Procedure also authorised the batlle to adopt certain measures in the framework of an investigation, including, under certain circumstances, requesting the interception of telephone calls.

The applicant was subsequently convicted and sentenced by a tribunal on 29 September 2015 for the sale and possession of large quantities of drugs for commercial purposes. The Andorran Higher Court of Justice upheld this judgment. That court noted that the first instance tribunal had before it several pieces of evidence which pointed to the applicant's guilt, including, amongst other evidence, the applicant's phone call records.

2. Decision of the Court

The applicant complained that the storage of data relating to his telephone communications and the use of that data in a criminal investigation amounted to an unjustified interference with his rights under Article 8 of the Convention. The applicant also complained that his rights under Article 6 had been violated.

Article 8

The impugned measure constituted an interference with the applicant's Article 8 rights. In relation to whether the interreference was prescribed by law, the Court did not consider it necessary to place emphasis on whether the applicant had given the telephone company permission to collect the data through agreeing to the telephone company's general terms and conditions. In any event, the interference was directly provided for by Article 87 of the State's Code of Criminal Procedure and Law no.15/2003 (the "Code").

The primary question in respect of whether the interference was prescribed by law, for the purposes of Article 8, was whether the effect of the national laws, being the storage and communication to the national court of the applicant's telephone data, and therefore the interference with the applicant's right to private life, was sufficiently foreseeable.

The Court referred to its previous case law and reiterated that in respect of the interception of communications, foreseeability cannot be assessed in the same manner as in other areas. In the context of surveillance, namely the interception of communications, foreseeability does not mean that an individual is able to foresee when the authorities can intercept their communications and to adapt their conduct accordingly. However, given the risk of arbitrariness when executive power is exercised in secret, particularly since the technology for the interception of communications continues to improve, the law must be sufficiently clear to indicate in a sufficient manner what circumstances and under what conditions public authorities may intercept communications. Further, the precision required by a national instrument, which cannot in any case provide for every eventually, depends to a considerable degree on the content of the instrument in question, the field it is designed to cover, and the number and status of those to whom it is addressed.

In the present case, the Court noted that Article 87 of the Code required the national courts to provide a reasoned decision explaining the necessity

and proportionality of any measure, considering the evidence obtained and the seriousness of the offence under investigation. The Court considered that the order of 30 August 2012 had complied with these requirements, having considered the needs of the investigation, the seriousness of the alleged offence and the practicalities of the intrusion into the applicant's private sphere.

Andorran law also provided several procedural safeguards against the exercise of arbitrary actions. These included that a judge's prior authorisation was required, there was a statutory time limit on the duration of the measures, the measures were only available for the most serious offences, and the applicant could at any time contest the lawfulness of the evidence gathered during the proceedings.

The Court also observed that the national law and rules drew no distinction between mobile telephone contract holders and users of prepaid telephone cards, and it was reasonable to consider that the national laws and rules were applicable to both.

The Court therefore concluded that the national law was sufficiently foreseeable for the purposes of Article 8(2).

The Court had no doubt that the interreference pursued a legitimate aim under Article 8(2), namely the prevention of crime. As regards the proportionality of the impugned measure, the Court highlighted that the measure had been authorised for a shorter period than that which the police had requested. Further, the alleged offences had been committed at most six months before the period covered by the measure. The Andorran authorities had respected the proportionality between the effects of the impugned measure and the objective of the prevention of crime, and they had used an unintrusive method to "enable the offence to be detected, prevented or prosecuted with adequate effectiveness". Accordingly, an appropriate balance had been drawn between the right to private life and the prevention of crime, and the Court found no violation of Article 8.

Article 6

In respect of Article 6, the applicant asserted that insufficient reasons had been provided in the domestic decisions, and the general terms and conditions of telephone contracts had been used in evidence before the Constitutional Court when this evidence had not been presented before the lower courts.

The Court reiterated that the obligation on tribunals to give reasons for their decisions did not require a detailed response to every argument. The Andorran courts had provided sufficient reasons. The Court was also clear that, although the Convention guarantees the right to a fair trial, it does not regulate the admissibility of evidence or its assessment which is primarily a matter for the national courts and domestic laws. The applicant had had the opportunity to contest the evidence presented before the Constitutional Court, and that court's decision could not be considered arbitrary or unreasonable.

The complaint under Article 6 was therefore rejected as manifestly ill-founded.

Comments made by the Interior Minister the day after the applicant's arrest giving the public the impression he was the head of a criminal group, and reasons given by the judge in ordering continued detention amounted to a declaration of guilt, both violated the presumption of innocence in Article 6

JUDGMENT IN THE CASE OF
GUTSANOVI v. BULGARIA

(Application no. 34529/10)
15 October 2013

1. Principal Facts

The four applicants were a well-known local politician, his wife, and their two minor daughters born in 2002 and 2004. The authorities suspected the first applicant of involvement in a criminal group accused of abusing power and embezzling public funds. Pre-dawn, around 6:30am, on 31 March 2010 a special team which included armed and masked police officers arrived at the applicants' home. A caretaker alerted them of the presence of the wife and children. After the first applicant not responding to the order to open the door, the police officers forced entry. The house was searched, and various items of evidence were taken. According to the applicants, masked police entered the bedroom where the parents had brought their children and threatened them with firearms and bright lights. After handcuffing the first applicant the police ordered the second applicant to cover her children with a duvet to prevent them from screaming and crying in fear. The police disputed this, claiming that they did not enter the bedroom to handcuff the first applicant, never spoke to the second, third and fourth applicants, and only entered the bedroom armed with tasers to help the first applicant to get dressed.

The first applicant was eventually arrested and escorted off the premises at 1pm, recorded by journalists and a television crew who had gathered outside the house. A press conference was held on the same day, during which the prosecutor announced that charges would be brought against the arrested individuals, including the first applicant, for their actions as part of a criminal group. At 10:55pm a prosecutor formally charged the first applicant with various offences and ordered his detention for seventy-two hours to ensure his attendance in court. On 1 April a newspaper published the prosecutor's speech, together with extracts of an interview with the Interior Minister, during which he referred to

the closeness of the first applicant with another suspect and their involvement in a "plot". On 3 April 2010, a tribunal placed him in pre-trial detention on the grounds that there was a risk that he might commit new offences. On 5 April 2010 the prime minister gave a live interview on current affairs, at the end of which he was asked to comment on the recent arrests. He mentioned the closeness of the first applicant with another suspect as well as their "material profit".

The first applicant's appeal against his pre-trial detention on 13 April 2010 and a further request for release on 18 May 2010 were rejected. On 25 May 2010 the Court of Appeal placed the first applicant under house arrest, noting that the danger of him committing new offences no longer existed. On 26 July 2010 the tribunal decided to release him on bail. At the time of the Court's judgment, criminal charges were still pending against the first applicant.

2. Decision of the Court

The applicants complained under Article 3 that they had been subjected to degrading treatment during the police operation at their home. The first applicant further complained under Articles 5 and 6 in relation to a number of issues, including that he had not been brought promptly before a judge and that the statements of public officials to the press had violated his presumption of innocence. Under Article 8 the applicants contended that the search carried out in their house constituted an unjustified interference with the right to respect for their home and family life, and under Article 13 that they had not had an effective remedy.

Article 3

The police operation was determined by the Court to have pursued the legitimate aim of carrying out an arrest and search in the general interest of the prosecution of criminal offences. However, the planning and execution of the police operation did not take into account several important factors, such as the nature of offences the first applicant was accused of, the fact that he did not have any violent history, and the presence of his wife and young children in the house. These factors indicated that the use of armed and masked agents, and the use of methods such as arriving very early in the morning, were excessive rather than what would have been strictly necessary to apprehend a suspect and gather evidence. The four applicants had been subjected to a psychological ordeal generating feelings of fear, anguish, and helplessness. The police actions were

therefore held by the Court to amount to degrading treatment for the purposes of Article 3, and constituted a violation of that Article.

Article 5

Article 5(3) – appearance before a judge

The first applicant was detained without trial for three days and six hours but was not required to participate in any investigatory measures after the first day. He was not suspected of involvement in any violent activity and was in a psychologically fragile state during the initial stages of detention following the degrading treatment he had suffered during the police operation, which had also been exacerbated by his public notoriety. Despite this notoriety he was also detained in the same city as the tribunal and did not benefit from any exceptional security measures. These elements led the Court to find a violation of the requirement in Article 5 to promptly present a suspect before a judge.

Article 5(3) – length of detention

The first applicant was detained for a period of 118 days (31 March to 30 July 2010), two months of which were under house arrest. The domestic tribunals' decisions to keep him in detention were based on the risk that he might commit a new offence, particularly interference with evidence. However, on 25 May 2010, the Court of Appeal decided that following the applicant's resignation from his post, this danger had passed. Yet, contrary to its obligations under domestic law, the same court placed the applicant under house arrest without offering any particular reason to justify this decision. Hence, the Court concluded that the authorities had failed in their obligation to provide pertinent and sufficient reasons for the first applicant's detention after 25 May 2010, and therefore had violated Article 5(3).

Article 5(5) – compensation

The State Liability Act did not provide the applicant with an effective remedy for the damages suffered by him during detention, as this required a formal finding by a domestic court that the detention had been unlawful. As the proceedings against the applicant were still pending, his detention was still considered lawful by the domestic courts and therefore the State Liability Act did not apply. Since no other domestic provision for compensation existed, the Court found that there had been a violation of Article 5(5).

Article 6

The Court examined the first applicant's claims that various public officials had violated his right to presumption of innocence. After finding no violation regarding the Prime Minister's interview and the prosecutor's conference speech, the Court went on to consider the implications of the Interior Minister's interview, during which he declared that what "[the first applicant and another suspect] have done represents an elaborate plot over a period of several years". The Court distinguished the nature of this interview, exclusively concerned with the police operation, from the spontaneous words of the Prime Minister several days later. In addition, the fact that this speech was published the day after the first applicant's arrest, and before the first applicant's appearance before a court, by a high government official, who in the circumstances should have taken precautions to avoid confusion, was significant. The words of the Interior Minister were more than a simple communication of information and suggested that the first applicant was guilty. Therefore there had been a violation of Article 6(2). Finally, the judge who rejected an application for release on 18 May 2010 stated that their court "remains of the view that a criminal offence was committed and that the accused was involved". This phrase was more than a mere description of suspicion, but was rather a declaration of the applicant's guilt before any decision on the merits of the case had been made. Consequently, this also breached Article 6(2).

Article 8

The Court noted that the search at issue was based on legislative provisions that posed no problem with regard to their accessibility and predictability for the purposes of the search being "in accordance with the law." As regards the last qualitative condition to be met by domestic legislation, namely compatibility with the rule of law, the Court recalled that in the context of seizures and searches it required that domestic law offer adequate guarantees against arbitrariness. In the instant case, the search of the applicants' house was carried out without a judge's prior authorisation. Such a search was permitted on the condition that a tribunal reviewed the search retrospectively to ensure that it met certain material and procedural conditions. In this case, the judge in question did not, however, give any reasons for his approval - he had simply signed and stamped the record followed by the word "approved". As a result, the Court considered that he did not demonstrate an effective control over the lawfulness and necessity of the search. Hence, the interference with the right to respect for home was not "prescribed by law" and therefore violated Article 8.

Article 13 in combination with Articles 3 and 8

No effective remedy existed in domestic law by which the applicants could assert their right not to be submitted to treatment contrary to Article 3 and to the right to respect for their home under Article 8. A violation of Article 13 in combination with these two Articles was therefore found.

Article 41

A joint sum of €40,000 was awarded to the applicants in just satisfaction and €4,281 for costs and expenses.

A public authority's use of secret interception of telephone calls made from a place of business, on an internal telecommunications system, without adequate warning, notice, or availability of domestic remedy or regulation, violated Article 8 and 13 of the Convention

JUDGMENT IN THE CASE OF

HALFORD v. THE UNITED KINGDOM

(Application no. 20605/92)
25 June 1997

1. Principal facts

The applicant was born in 1940 and resided in the Wirral. From 1962 until 1992 she worked in the police service.

In May 1983 the applicant was appointed Assistant Chief Constable with the Merseyside police. Upon her promotion, the applicant was provided with her own office and two telephones, one for professional, and one for private use. Both telephones were part of the department's internal telephone network, and were not subject to public telecommunications laws. The applicant was not given any specific restrictions nor guidance as to the use of the telephones.

Over the course of the following seven years, the applicant repeatedly applied to be appointed to the rank of Deputy Chief Constable. This promotion was under the discretion of the Home Office. Per the applicant, the Chief Constable of Merseyside disapproved of women in leadership, and intervened to deny the applicant her requisite Home Office approval. After receiving another promotion refusal in February 1990, the applicant commenced proceedings against the Chief Constable and the Home Secretary, formally alleging discrimination on the basis of sex.

In June 1990, a "Special Committee" was appointed to address the discrimination allegations. The applicant alleged that the Police Authority then launched a retaliatory campaign against her, which included actions such as interception of her personal telephone calls, for the purposes of obtaining information to use against her in the discrimination proceedings, as well as disciplinary action. In September 1990, the disciplinary proceedings culminated in the form of a written report alleging misconduct on the part of the applicant. In December 1990, the

applicant was suspended from duty. In early 1991, the Disciplinary Committee resolved to formally press charges.

Ultimately, the charges were quashed due to probable unfairness on the part of the authorities. The applicant accepted a settlement in July 1991, and agreed to retire thereafter, ostensibly for unrelated reasons. The Home Office agreed to implement various Equal Opportunities Commission proposals, and to review its selection procedures for police posts.

The Commission[265] declared the application admissible on 2 March 1995, finding that there had been violations of Articles 8 and 13 in relation to the interception of the applicant's telephone calls from her office telephone. While the Government conceded before the Commission that the applicant had established, through compiled evidence, a reasonable likelihood that her office phone calls had been intercepted, they declined to find so for her home phone. This determination was upheld by two tribunals, as well as the Home Secretary, either in affirmative agreement with the Government's determination, or as the result of jurisdictional limitations. The Commission likewise found no violation for the remainder of the applicant's complaints, including Article 8 and 13 in relation to her home telephone, Article 10 in relation to her office telephones, and Article 14 in relation to the alleged sex discrimination.

2. Decision of the Court

The applicant complained that the interception of her telephone calls from both her home and office telephones had violated her Article 8 and 10 rights to respect for her private life, and freedom of expression, respectively. The applicant further complained that her Article 13 right to an effective remedy had been violated, as well as her Article 14 right to be free of discrimination.

Article 8

The Court noted that phone calls made from both an applicant's business, as well as from their home, were covered by notions of "private life" and "correspondence" within the meaning of Article 8. Because the applicant had

[265] From 1954-1998 the European Commission of Human Rights (Commission) acted as an intermediary between individual applicants and the European Court of Human Rights. Upon the passage of Protocol 11, the Commission was abolished, in favour of direct access to the Court.

not received any notice of her telephones being subject to monitoring, it was reasonable to have expected her calls would remain private. This expectation was reinforced by the fact that her office was designated for her private use, as well as by reassurance on the part of the authorities that she could use her office telephone for calls related to the sex-discrimination proceedings.

Moreover, the applicant had adduced evidence establishing a reasonable likelihood that her office calls had been intercepted in order to gather material to defeat her discrimination claims. For the interference to have been justified, it had to have been "in accordance with the law," complying both with existing domestic law, and with general notions of the rule of law. To meet this standard, the authorities must have provided adequate notice of the circumstances under which authorities were empowered to resort to secret measures against citizens. No such provisions existed in domestic law for telephone calls made on internal communications systems.

As for the applicant's home telephone, the Court first distinguished the cases of Klass[266] and Malone[267] in that the applicant's Article 8 rights were not menaced by the mere existence of secret surveillance measures; rather, she was allegedly subject to such measures, in an unlawful manner. However, the Court found that the applicant's evidence of interference with her home telephone were speculative and insufficient to establish a reasonable likelihood of interference.

While the applicant's home and office telephones alike were protected under Article 8, the Court could only find a reasonable likelihood of interference with the applicant's office telephone. With no legal standards preventing the abuse of power in relation to the applicant's office calls, the Court found the interceptions to not be in accordance with the law, in violation of the applicant's Article 8 rights to private and family life.

Article 13

The Court acknowledged that the applicant was entitled to an effective remedy for the violation of her Article 8 rights, in relation to the interception of her office

[266] *Klass and Others v. Germany*, judgment of 8 September 1978, no. 5029/71, also included as a summary in this publication.

[267] *Malone v. the United Kingdom*, judgment of 2 August 1984, no. 8691/79, also included as a summary in this publication.

telephone calls. Because there were no domestic laws regulating the interception of calls made on internal communications systems generally, nor those operated by public authorities such as the Merseyside police, the applicant was unable to seek legal relief.

As it related to the applicant's home telephone calls, the Court called attention to the fact that an "interference" within the meaning of Article 8 required a reasonable likelihood that the applicant had been subject to surveillance. The Court reiterated that it had previously found the applicant's evidence in this regard insufficient.

The Court therefore found no violation of the applicant's Article 13 right to effective remedy in relation to the applicant's home telephone complaint, but did find there had been a violation in relation to the interception of her office telephone calls.

Articles 10 and 14

The Court considered the applicant's allegations in relation to Articles 10 and 14 to be duplicative of her complaints under Article 8, and therefore found it unnecessary to examine them separately.

Article 50 (now Article 41)

The Court awarded the applicant €10,600 in respect of pecuniary and non-pecuniary damage, and €25,000 for costs and expenses.

Practically unfettered power exercised by national intelligence service in the implementation of a surveillance operation, and retention of data governed by confidential rules, amounted to a violation of the applicant's right to respect for private life under Article 8

JUDGMENT IN THE CASE OF
HAŠČÁK v. SLOVAKIA

(Application nos. 58359/12, 27787/16 and 67667/16)
23 June 2022

1. Principal facts

The applicant was born in 1969 and lived in Bratislava. The three applications originated from various facts linked to a public corruption surveillance operation carried out in 2005 and 2006 by the Slovak Intelligence Service ("the SIS") which had been authorised by two warrants issued by the Bratislava Regional Court ("the BRC"). The surveillance was conducted with the aim of monitoring the private dealings of Mr Zoltán Varga and an unnamed associate, who the applicant submitted was him. In 2011, the existence of that operation became publicly known by its codename of "Gorilla" when some of the material allegedly linked to the operation was anonymously posted on the internet. The Court adjudicated related claims made by Mr Varga in Zoltán Varga v. Slovakia.[268]

In 2012, the Constitutional Court in Slovakia ruled in favour of Mr Varga in an action that he brought regarding the Gorilla investigation, subsequently annulling the initial warrants because of the BRC's mishandling of the investigation, resulting in a violation of Mr Varga's privacy rights. The actual primary surveillance materials had already allegedly been deleted in 2008, but the derivative materials, which may have consisted of materials such as summaries, notes and analytical documents, continued to be maintained by the SIS – a maintenance which the Constitutional Court determined it did not have the jurisdiction to alter. By law, the derivative material could only be accessed by a competent court.

When the materials from the Gorilla investigation were anonymously posted online in 2011, the applicant noted that his name was mentioned in the materials more than 800 times. The applicant made requests to delete any materials

[268] *Zoltán Varga v. Slovakia*, judgment of 20 July 2021, nos. 58361/12, 25592/16 and 27176/16.

related to the investigation to various government bodies which were futile since there was no organ hierarchically superior to the SIS. Several months later, the Minister of the Interior informed the public that the Gorilla investigation was in fact an ongoing SIS investigation and that some of the materials online had been verified as being from that investigation. The government repeatedly updated the public on the status of the ongoing investigation into public corruption. No charges were formally brought against the applicant. Through various domestic legal proceedings, the applicant repeatedly challenged the State's decision to arbitrarily involve him in the investigation and requested access to and the deletion of the surveillance materials that involved him.

2. Decision of the Court

Relying on Article 6 (right to a fair trial), and Article 8 (right to respect for private life), the applicant complained, in particular, that there had been a lack of effective supervision and review of the implementation of the two surveillance warrants, that the applicable framework provided no protection to individuals randomly affected by surveillance measures, and that the internal rules applicable to the retention of intelligence material were inadequate.

Article 8

Firstly, considering the scope of the case, the Court noted that it involved no complaint of any leak of information by the SIS and no complaint concerning the practical and procedural status of the audio recording retrieved by the investigators in 2018.

It was undisputed that the applicant was subjected to surveillance on the basis of the two warrants and that various items of material arising from their implementation and at least in part concerning him were still retained by the SIS and the BRC at the time of the Court's judgment. The Court found that the implementation of the warrants and the retention of gathered material was an interference with the applicant's right to respect for private life within the meaning of paragraph 1 of Article 8.

To determine whether the interference entailed a violation of Article 8 of the Convention, the Court had to examine whether it was "in accordance with the law", pursued one or more legitimate aims as defined in the second paragraph of that Article and was "necessary in a democratic society" to achieve such aim

or aims. Regarding the phrase "in accordance with the law", the Court's case law requires the examination of whether the interference complied with domestic law and whether the domestic law itself is compatible with the rule of law. To comply with the rule of law, laws must provide a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 of Article 8. Secretly exercised executive power poses a risk of arbitrary administration. Since the implementation in practice of measures of secret surveillance is not open to scrutiny by the individuals concerned or the public at large, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference or unfettered exertions of executive power.

Regarding the implementation of the warrants, the Court found that the conclusions made in Zoltán Varga were directly applicable in the present case. As such, the Court determined that – in view of the lack of clarity of the applicable jurisdictional rules and the lack of procedures for the implementation of the existing rules and flaws in their application (these deficiencies were found by the Constitutional Court and attributed to the BRC, the court which issued the warrants) – when implementing the warrants the SIS had practically enjoyed discretion amounting to unfettered power, which had not been accompanied by a measure of protection against arbitrary interference, which meant that the implementation of the warrants was not "in accordance with the law" for the purposes of Article 8 § 2 of the Convention. The situation in the present case was further aggravated by two additional factors. First, there had been no indication that the 2005 warrant actually targeted the applicant, leading to the plausibility of the idea that he was randomly affected by the government's arbitration exertion of its surveillance powers. Second, there was a protracted fundamental uncertainty in the applicable legal framework as to the practical and procedural status of the presumably leaked primary material from the implementation of the two warrants.

Regarding the storing of the derivative material from the implementation of the warrants, the Court once again found that the conclusions made in Zoltán Varga were directly applicable in the present case. As such, the Court determined that the retention of derivate material from the implementation of the warrants was not maintained "in accordance of the law" because the retention of the material was governed by confidential rules which had been both adopted and

applied by the SIS, with no element of external control. These rules had been lacking in accessibility and had provided the applicant with no protection against arbitrary interference with his right to respect for his private life.

Given the implementation of the two warrants and the retention by the SIS of the derivative material from their implementation, the Court found that there had been a violation of the applicant's right under Article 8 of the Convention to respect for his private life.

Article 6

For a complaint to fall within the material scope of Article 6, the applicant must have been charged with a criminal offence. The Court found that neither the impugned public statements nor any other circumstance indicated by the applicant had placed him in the position of a person who has been charged with a criminal offence. Consequently, the Court determined that the applicant's Article 6 complaints fell outside the scope of the Convention ratione materiae.

Article 41

The Court awarded the applicant €9,750 in respect of non-pecuniary damage.

The recording of a conversation using a body-mounted listening device and the interception of telephone calls, and the subsequent use of the information obtained in criminal proceedings, violated Article 8 but did not violate Article 6

JUDGMENT IN THE CASE OF
HEGLAS v. THE CZECH REPUBLIC

(Application no. 5935/02)
1 March 2007

1. Principal facts

The applicant was born in 1976 and lived in the Czech Republic. The applicant was arrested and found guilty, along with another (referred to as A.M.), of robbery. Among other evidence the Prague City Court's judgment was based on (1) a list of telephone calls between the applicant and A.M. (the "call list"); and (2) a transcript of a conversation between the applicant and another individual (A.B.), which was recorded by A.B. wearing a police-fitted recording device, during which the applicant admitted that he had organised the robbery with A.M. (the "transcript"). The first instance court described the latter as crucial evidence.

The applicant and A.M. appealed the first instance court's decision, including on the basis of the illegality of the transcript and the call list. The Prague High Court dismissed the appeals. The Constitutional Court also dismissed the applicant's appeal based on Articles 6 and 8 of the European Convention on Human Rights. That court held, among other considerations, that the applicant had been convicted based on several pieces of evidence whose substantiation and assessment were not open to doubt.

The court considered that the use of the listening device was not prohibited under the Code of Criminal Procedure ("CCP"), but that the transcript should not have been used as evidence in the criminal proceedings. However, this did not mean that the decisions adopted in those proceedings were unconstitutional as the applicant's conviction was based on several pieces of evidence.

2. Decision of the Court

The applicant complained that the secret recording of his conversation with A.B. and the interception of a list of telephone calls, and the subsequent use of

both as evidence in the criminal proceedings, violated his rights under Articles 8 and 6 § 1 of the Convention.

Article 8

As regards the use of the list of telephone calls between the applicant and A.M. (the call list), the Court considered, in line with its previous case law, that the covert interception of telephone calls, including information on the dates of phone calls, numbers called or calls received, and the length of telephone conversations, engaged Article 8. The use of the call list as evidence in criminal proceedings therefore interfered with the applicant's right to respect for private life under Article 8.

The central question was whether the interference was in accordance with the law as required by Article 8 § 2. The Court observed that the interception and recording of the telephone conversations had been ordered by a district judge from 21 January to 21 February 2000 under the CCP. The list of calls in question had also been produced at the request of the police in accordance with the provisions of the CCP and of the Telecommunications Act (the "Act"). However, the relevant provisions of the CCP and the Act had not entered into force at the material time. Article 88a of the CCP and section 84(7) of the Act, the provisions which authorised the criminal investigation authorities to obtain lists of telephone calls, only entered into force on 1 January 2002 and 1 July 2000, respectively.

Further, even if domestic law did provided a legal basis for the interception of telephone calls, the domestic courts had been supplied with a list of calls starting on 19 January 2000, so two days before the dates permitted under the district judge's order.

The interreference therefore had not been in accordance with the law and Article 8 had been violated. There was no need to consider whether the interference was justified.

As regards the secret recording of the conversation between the applicant and A.B. and the subsequent use of the transcript as evidence in criminal proceedings, the Court held that this interfered with the applicant's right to respect for private life under Article 8.

The Court considered that the recording and use of the transcript was not authorised by a law which satisfied the criteria laid down by the Court's case-law. The recording had been undertaken pursuant to a practice which could not be regarded as having a specific legal basis with sufficiently precise conditions for when such an interference could occur, including as regards the admissibility, scope, control, and use of any information collected.

The Court concluded that it had not been demonstrated that the interference was in accordance with the law, and Article 8 had been violated. There was no need to consider whether the interference was justified.

Article 6

The applicant contended that the use of the transcript and the call list as evidence in the criminal proceedings interfered with his right to a fair trial. He noted that the domestic Constitutional Court had found in a different case that it was unlawful to use a list containing information on telephone calls as evidence.

The Court recalled, referring to its previous case law, that although Article 6 guarantees the right to a fair trial, it does not regulate the admissibility of evidence which is primarily for domestic law. The Court will therefore not, in principle, pronounce on the admissibility of certain types of evidence, including evidence which may have been obtained unlawfully under domestic law. Rather, the Court will examine whether the procedure, including the manner in which the evidence has been obtained, was fair as a whole. This requires an examination of the unlawfulness in question and, where applicable, the nature of any violation of another Convention right. In doing so, the Court will also consider whether the accused's rights of defence have been respected, including if the accused was afforded the possibility to put into question the authenticity of the evidence and to oppose its use in the proceedings. The public interest in the prosecution of the offence and the criminal sanction, can also be considered and balanced against the interests of the accused. However, the public interest cannot justify measures which impair the very essence of the right to a fair trial.

In the present case the Court noted that before the first-instance court, and then before the High Court and the Constitutional Court, the applicant was able to raise all the necessary observations on the transcript and the call list. The applicant therefore had been convicted following adversarial proceedings. Moreover, the transcript and the call list, although considered the most important

or essential evidence by the first instance court, were not the sole evidence upon which that court had based its decision. In relation to the public interest in the use of such evidence to obtain the applicant's conviction, the Court observed that the measures had been taken against a person who had committed a serious harm offence, and who had subsequently received a nine-year prison sentence.

The Court concluded that the use of the transcript and the call list in the domestic criminal proceedings had not infringed the applicant's right to a fair trial.

Article 41

The Court did not award the applicant damages for pecuniary or non-pecuniary damage, and considered that the findings of violations constituted sufficient just satisfaction. The Court awarded the applicant €1,018 for costs and expenses.

An order to anonymise an offender's identify in an article in a newspaper's electronic archive on the grounds of the "right to be forgotten" did not violate Article 10

GRAND CHAMBER JUDGMENT IN THE CASE OF
HURBAIN v. BELGIUM

(Application no. 57292/16)
4 July 2023

1. Principal facts

The applicant was born in 1959 and lived in Belgium. He was the publisher of Le Soir, a Belgium daily newspaper. A 1994 print edition of Le Soir included an article reporting on several car accidents, including an accident that caused the death of two people and injured three others (the article). The article mentioned the full name of the driver responsible (referred to as G). G was convicted in 2000. He served his sentence and was rehabilitated in 2006.

In 2008, Le Soir placed on its website an electronic version of its archives, including the article. In 2010, G asked Le Soir to remove the article from its electronic archives or at least anonymise it, which Le Soir refused to do. G's request mentioned his profession as a doctor and that the article appeared among the results when his name was entered into search engines. G subsequently brought proceedings against the applicant, in his capacity as editor of Le Soir, seeking to obtain the anonymisation of the article. The proceedings were founded on the right to private life, which, under Belgium law, encompassed the "right to be forgotten".

In 2013, the Belgian tribunal of first instance granted most of G's claims. In 2014, the Court of Appeal of Liege upheld this. The applicant's appeal to Court of Cassation was dismissed in 2016. The domestic courts made orders requiring the applicant to anonymise the article.

2. Decision of the Court

The applicant complained that the civil judgments ordering him to anonymise the archived version of the article violated his rights under Article 10 of the Convention. In its judgment of 22 June 2021, a Chamber of the Court held that there had been no violation of Article 10. At the applicant's request, under Article 43, the case was referred to the Grand Chamber.

Article 10

It was not in dispute that the anonymisation order interfered with Article 10. The Grand Chamber also agreed with the Chamber's findings that the interference was in accordance with law. It was not disputed by the parties that the interference was for a legitimate aim, namely G's right to respect for his private life under Article 8. The Court was therefore concerned with whether the interference was necessary in a democratic society.

The Court was only concerned with the version of the article placed on Le Soir's website. It was the continued availability of the information on the internet, rather than its original publication per se, that was in issue. The Court also emphasised that the original printed article had been published in a lawful and non-defamatory manner.

The Court reiterated its case law as to the importance of freedom of expression and on the role of the press, which includes maintaining news archives. Internet / digital archives make a substantial contribution to preserving, and making available to the public, news and information, as well as being an important source of education and historical research. Archives should, in general, remain authentic, reliable and complete. This requires the press to have comprehensive records. The Court considered that the integrity of digital press archives should be the guiding principle underlying any request for the removal or alteration of all or part of an archived article, especially if the lawfulness of the article has never been questioned.

In respect of the "right to be forgotten", the Court recognised that an individual who is the subject of an online article will have an interest in obtaining the erasure or alteration of, or the limitation of access to, information in the article. Personal information that is on the internet for some time may have far-reaching negative impacts, e.g. on public opinion or when an individual applies for a job. The "right to be forgotten" has been linked in the Court's case law to Article 8, namely to respect for reputation. It is not a self-standing right under the Convention and will only be covered by Article 8 in certain situations and for certain information.

The Court also considered wider judicial practice on the "right to be forgotten", including in national legal systems and in European Union ("EU") law. In respect of EU law, the Court noted the decisions of the Court of Justice of the European

Union in Google Spain[269], and subsequent cases on the "right to be forgotten", namely in relation to the operations carried out by a search engine. The Court, amongst other matters, noted how the Google Spain judgment highlighted the importance of the protection of personal data, the impact on an individual's private life of the continued availability of data online, and the amplifying effect of search engines, as well as the different considerations that may apply to requests to search engines as opposed to the website publisher.

The Court considered that, in view of the fact that the case concerned an electronic archived article rather than initial publication, the criteria previously developed for addressing a conflict between the rights under Articles 10 and 8 had to be adjusted. In the context of a request to alter journalistic content that is archived online the following criteria should be considered: "(i) the nature of the archived information; (ii) the time that has elapsed since the events and since the initial and online publication; (iii) the contemporary interest of the information; (iv) whether the person claiming entitlement to be forgotten is well known and his or her conduct since the events; (v) the negative repercussions of the continued availability of the information online; (vi) the degree of accessibility of the information in the digital archives; and (vii) the impact of the measure on freedom of expression and more specifically on freedom of the press." The Court also observed that search engines and the publisher website are different forms of processing. Data subjects should not be obliged to contact the website to be able to exercise their rights in relation to search engines, and vice versa.

With regards to the present case, the Court reiterated its case law on the margin of appreciation left to national authorities in resolving a conflict between Articles 8 and 10. The Liège Court of Appeal had taken into account several criteria in the reasoning of its decision. If that court's assessment was consistent with the criteria that the Court had identified (as set out above), the application of which must also consider the specific characteristics of cases concerning the alteration of online archives, the Court would require strong reasons to substitute its own views for that of the domestic court.

As to the nature of the archived information, it was necessary to ascertain whether the information related to the private, professional or public life of the person concerned, and whether it had a social impact or instead fell within the

[269] *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (judgment of 13 May 2014, C-131/12, EU:C:2014:317).

intimate sphere of private life. Although data concerning criminal matters had been classified as "sensitive", the Court noted that information about the person concerned is an important aspect of press articles about criminal proceedings. In the present case, the Court agreed with the findings of the Liège Court of Appeal that the facts reported in the article were of a judicial nature. This is since the facts reported related to facts which subsequently gave rise to a criminal conviction. However, the Court was of the view that the facts were not in a category of offences whose significance, owing to their seriousness, was unaltered by the passage of time. The Court also observed that the events did not attract widespread publicity, with the only media coverage being the article in question (a factor which the Liège Court of Appeal had also considered).

As to the time that had elapsed since the events and since the initial and online publication, the relevance of information would be linked to its topicality. The Court agreed with the Liège Court of Appeal that the passage of a significant length of time would be relevant. In the present case, sixteen years had elapsed between the initial publication of the article and the first request for anonymisation. G had been rehabilitated in 2006 and he had a legitimate interest in being reintegrated into society.

As to the contemporary interest of the information, this could include whether the article continued to contribute to a debate of public interest, if it had any historical, research-related or statistical interest, and whether it remained relevant so as to place recent events in context. Public interest however does not equate to the public's thirst for information about the private life of others. In the present case, the Court saw no reason to question the reasoned assessment of the Liège Court of Appeal that the article merely made a statistical contribution to a public debate on road safety and had no historical significance since the news story, albeit tragic, was not alleged, nor demonstrated, to have been a source of particular public concern.

As to whether the person claiming the entitlement to be forgotten is well known, and his or her conduct since the events, the Court noted the importance of this criterion. The extent to which an individual has a public profile, assessed at the time the request is made, influences the protection to be given under Article 8. A person's conduct may also both justify refusing a "right to be forgotten" request or may weigh in its favour. In the present case, the Liège Court of Appeal had observed that G did not hold any public office, and considered that the mere fact that G was a doctor did not justify his continued identification in the article.

The Court agreed with the Liège Court of Appeal and also noted that G was not a public figure, the case had never attracted widespread publicity, and there was nothing to suggest that G had tried to publicise his situation; on the contrary, all of G's conduct demonstrated a desire to stay out of the media spotlight.

In respect of the negative repercussions of the continued availability of the information online, a person requesting the alteration of an article stored on a digital press archive must be able to make a duly substantiated claim of serious harm to their private life. In respect of judicial information, the impact of its continued availability to a person's reintegration into society will be relevant. It should be ascertained whether the person's conviction has been removed from the criminal records, though the fact that a person has been rehabilitated cannot by itself justify a "right to be forgotten" request. In the present case, the Liège Court of Appeal had observed that a search based on G's name on search engines would bring up the article. This made knowledge of G's conviction readily accessible to a wide audience, which, since G was a doctor, would include patients, colleagues and acquaintances. This, in the Liège Court of Appeal's view, was undoubtedly a source of harm to G. The Court saw no strong reason to call into question the reasoned decision of the Liège Court of Appeal on this criterion.

Regarding the degree of accessibility of the information in the digital archives, the Court reiterated that while internet sites are an information and communication tool distinct from print media and posing a higher risk of harm, generally consulting archives requires an active search on a dedicated web page. However, in the present case, as the domestic courts had observed, the digital archives of Le Soir were available free of charge and there was a high degree of accessibility. The Court therefore saw no strong reason to call into question the reasoned decision of the Liège Court of Appeal that, in light of the high degree of accessibility, the continued Prescence of the article in the archives undoubtedly caused harm to G.

As to the impact of the measure on freedom of expression and freedom of the press, the Court noted the development of various measures aimed at protecting the reputation and rights of others in respect of information in the digital sphere. In view of the importance of the integrity of digital press archives, preference should be given to the measure that is both best suited to the aim pursued, assuming it to be justified, and least restrictive of press freedom. In the present case, the Liège Court of Appeal had found that the most effective means of protecting G's privacy, without interfering disproportionately with the applicant's freedom of expression,

was to anonymise the article. Other means (e.g. adding further information to the article or requiring search engines to delist it) were either inappropriate, not possible or had not been requested by the applicant in the lower courts. The Court also noted its previous case law that recognised that anonymisation is generally less detrimental to freedom of expression than the removal of an entire article. Further, the Liège Court of Appeal had taken care to assess the implications of the measure for G, the public and for the applicant. That court had also taken into account the importance to be attached to the integrity of the archives. The Court added that the Liège Court of Appeal's decision was on the anonymisation of the online archived version alone and that the paper archives remained intact and could be consulted by any interested person.

As regards the possible chilling effect on freedom of press, the Court considered that an obligation to anonymise an article that had been lawfully published may in principle fall within the duties and responsibilities of the press. In any event, it did not appear that the anonymisation order had impaired Le Soir's ability to perform its journalistic tasks.

The Court concluded that having regard to the margin of appreciation, the national courts had carefully balanced the rights at stake in accordance with the Convention and had taken into account, in a coherent manner, the relevant criteria. The national courts had concluded that the interference with the freedom of expression of the applicant had been limited to what was strictly necessary and could, in the circumstances of the case, be regarded as necessary in a democratic society and proportionate. The Court saw no strong reasons to substitute its own view for that of the national courts or disregard the outcome of the balancing exercise carried out by them.

Secret surveillance measures did not violate with the right to respect for private life; restrictions in the procedure for challenging such measures did not breach the right to a fair trial

JUDGMENT IN THE CASE OF

KENNEDY v. THE UNITED KINGDOM

(Application no. 26839/05)

18 May 2010

1. Principal facts

The applicant was born in 1946 and lived in the United Kingdom. He claimed that his business mail, telephone and email communications were being intercepted by the United Kingdom government agencies, and that this was because he had been the subject of a high-profile criminal case and had subsequently campaigned against miscarriages of justice.

The applicant brought proceedings in the Investigatory Powers Tribunal ("IPT") complaining that his communications were being intercepted. He also asked for the proceedings to be conducted in a certain way to ensure their fairness, including an oral hearing in public, and the mutual inspection of witness statements and evidence between the parties.

The IPT ruled that no determination had been made in the applicant's favour, meaning that either there had been no interception, or any interception had been lawful.

2. Decision of the Court

The applicant complained that the alleged interception of his communication violated his rights under Article 8 of the Convention. He further complained that the United Kingdom legislative regime, namely the Regulation of Investigatory Powers Act 2000 ("RIPA"), was incompatible with Article 8. In addition, he complained that the hearing before the IPT did not have adequate safeguards and thus violated his rights under Article 6 to a fair trial. He also complained that he had been denied an effective remedy, as required by Article 13.

Article 8

The Court first held that the complaints on Article 8 were admissible, even though the applicant had failed to raise his arguments as regards the overall Convention-compatibility of RIPA before the IPT. For a State to claim non-exhaustion of remedies, they must satisfy the Court that the remedy proposed was an effective one. Although the IPT could have made a general public ruling on the compatibility of RIPA with the Convention, it was not clear what benefit, if any, could be obtained from such a ruling since the RIPA provisions were primary legislation. The applicant therefore was not required to have advanced before the IPT his complaint on the general compliance of RIPA with Article 8.

Moving on to consider the merits of the applicant's complaint, the Court reiterated that where an applicant complains that their communications have been intercepted, the Court must be satisfied that there is a reasonable likelihood that this did occur. The Court will make its assessment in light of all the circumstances and direct proof that surveillance has taken place is not necessarily required. Where the Court is considering whether an applicant can claim an interference due to the existence of legislation permitting surveillance, the Court will consider the availability of any remedies and the risk of secret surveillance measures being applied to the applicant. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, even where the actual risk of surveillance is low, there is a greater need for scrutiny by the Court.

In the present case, the applicant's complaints that calls were not put through to him and that he received hoax calls, did not demonstrate a reasonable likelihood that there was actual interception of his communications. However, given the applicant's allegations that interception was taking place to intimidate him, it could not be excluded that he had been subject to, or at risk of being subject to, secret surveillance measures.

As regards the justification for the interference, the Court noted that States enjoy a margin of appreciation. However, the Court has a supervisory role in determining whether the procedures for supervising the ordering and implementation of the interception measures are sufficient to keep the "interference" limited to what is "necessary in a democratic society".

The Court noted that the interreference, if it occurred, would pursue the legitimate aims of protecting national security and the economic well-being

of the country and preventing crime, as set out in RIPA, supplemented by the Interception of Communications Code of Practice (the "Code"). The United Kingdom regime defined with sufficient precision the cases where interception would be permitted; an exhaustive list of the national security offences where interception of communications may occur was not required.

As to the categories of persons targeted, the Court noted that although under RIPA it was possible for the communications of any person in the UK to be intercepted, a warrant which clearly specified, either by name or by description, the interception subject, was required. The indiscriminate interception of vast amounts of communication was not permitted. RIPA also clearly indicated the time period under which an interception warrant would expire and the conditions under which a warrant could be renewed, which also required the authorisation of the Secretary of State. The duration of any interception measures would depend on the complexity and duration of the investigation and, provided that adequate safeguards existed, it was not unreasonable to leave the matter for the discretion of the domestic authorities.

As regards the procedure for examining, using and storing data, and the processing and communication of intercepted material, RIPA and the Code contained several safeguards. Under RIPA any data obtained had to be stored securely and there were provisions regulating its communication. The Code imposed various restrictions, including procedures on storing data securely, strictly limiting the number of persons to whom intercept material could be disclosed, requiring persons to have security clearance to access the data, requiring that data should only be communicated where there was a "need to know" and, where possible, requiring only summaries to be disclosed. Intercepted material, and any copies, also had to be destroyed as soon as there were no longer any grounds for its retention, and reviews were to occur at appropriate intervals.

There was also sufficient supervision of the RIPA regime. An Interception of Communications Commissioner, who was independent from the executive and the legislature, was tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. Any person who suspected that their communications had been or were being intercepted could also apply to the IPT, which was an independent and impartial body, and which had access to closed material.

The Court therefore concluded that the domestic law indicated with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of any intercept material collected. There was also no evidence of any significant shortcomings in the application and operation of the surveillance regime. Considering the safeguards in place, any surveillance measures, if they had been applied to the applicant, would have been justified under Article 8 § 2.

Article 6 § 1

The Court first considered that, in the present case, it was not necessary for it to reach a conclusion on whether the proceedings concerned "civil rights and obligations" such that Article 6 would apply, as, in any event, the Court considered that the IPT's rules of procedure complied with the requirements of Article 6 § 1.

The Court reiterated that, in both criminal and civil proceedings, the right to a fully adversarial procedure can be limited where necessary in the light of a strong countervailing public interest, such as national security. Any difficulties caused to the defendant must however be sufficiently counterbalanced by the procedure adopted. The Court emphasised that the need to keep secret sensitive and confidential information justified restrictions in the IPT proceedings. However, the question was whether the restrictions, taken as a whole, were disproportionate or impaired the very essence of the applicant's right to a fair trial.

The Court recalled that there is no absolute right to the disclosure of relevant evidence. In the present case, the Court agreed with the United Kingdom government that it was not possible to disclose redacted documents or to appoint special advocates as this would not have preserved the secrecy of whether any interception had taken place. The obligation to hold a hearing is not absolute, and national security can justify the public's exclusion from proceedings. The duty to give reasons may also vary according to the decision and circumstances of the case. In the context of the IPT proceedings, the Court considered that it was sufficient that a complainant would be advised that no determination had been made in their favour, and, if they were successful a complainant was also entitled to information regarding the findings of fact.

The Court concluded that the restrictions on the procedure before the IPT were necessary and proportionate to the need to ensure the efficacy of the secret surveillance regime and did not impair the very essence of the applicant's right to

a fair trial. In reaching this conclusion, the Court emphasised the breadth of access to the IPT for those complaining about interception, including the absence of any evidential burden to lodge a complaint.

Article 13

Given its conclusions in respect of Article 8 and Article 6, the Court considered that the IPT provided the applicant with an effective remedy in so far as his complaint concerned the alleged interception of his communication. In respect of the applicant's general complaint that the regime breached his rights under Article 8, the Court reiterated that Article 13 does not require an effective remedy where the alleged violation arises from primary legislation. There had accordingly been no violation of Article 13.

The use of an unlawfully obtained audio recording and the lack of an effective domestic remedy constituted violations of Articles 8 and 13, but not of the applicant's Article 6 rights

JUDGMENT IN THE CASE OF

KHAN v. THE UNITED KINGDOM

(Application no. 35394/97)

12 May 2000

1. Principal facts

The applicant arrived at Manchester Airport on a flight from Pakistan on 17 September 1992 along with his cousin, N., who was found to be in possession of heroin with a street value of almost £100,000. N was interviewed and then arrested and charged. No drugs were found on the applicant, and he was released without charge. On 26 January 1993 the applicant visited a friend, B., in Sheffield. B. was under investigation for dealing in heroin. On 12 January 1993 the installation of a listening device on B.'s premises had been authorised by the Chief Constable of South Yorkshire on the grounds that the conventional methods of surveillance were unlikely to provide proof that he was dealing in heroin. By means of the listening device, the police obtained a tape recording of a conversation in which the applicant admitted that he had been a party to the importation of drugs by his cousin N. on 17 September 1992. The applicant was arrested on 11 February 1993, and he and N. were jointly charged with offences under the Customs and Excise Management Act 1979 and the Misuse of Drugs Act 1991. During the trial, the applicant admitted that he had been present at the Sheffield address and that his voice was one of those recorded on the tape. Although the Government accepted that without the recording there was no case against the applicant, the trial judge ruled that the evidence was admissible, and on 14 March 1994 the applicant was sentenced to three years' imprisonment. The applicant appealed to the Court of Appeal on the ground that the evidence ought to have been held to be inadmissible. After this appeal was dismissed, the applicant appealed to the House of Lords, which also dismissed his appeal.

2. Decision of the Court

The applicant complained that his rights under Article 8 had been violated by the usage of a covert listening device to record the private conversation that he

took part in at B.'s premises. He also complained that there had been a violation of his right to a fair trial under Article 6, on the ground that the sole evidence in his case was material which had been obtained in breach of Article 8, and was therefore not compatible with the "fair hearing" requirement. Finally, the applicant complained that his right to an effective remedy had been violated in breach of Article 13, on the ground that the domestic courts should have taken into account that the evidence had been obtained in breach of the Convention.

Article 8

The Court stated that the principal issue in the case was whether the interference was justified under Article 8 § 2, which would be determined by consideration of whether it satisfied the two criteria of being "in accordance with the law" and "necessary in a democratic society". In its consideration of these two criteria, the Court noted that in the context of covert surveillance by public authorities the relevant domestic law must provide protection against any arbitrary interference with an individual's rights under Article 8. Under the "foreseeability" requirement, the law must also be sufficiently clear to provide the public with an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to the use of covert measures.

Concurring with previous case law, the Court noted that at the time there was no domestic law or statutory system regulating the use of covert listening devices, and that the Home Office Guidelines were neither legally binding nor directly publicly accessible. Hence, the Court found that the interference could necessarily not be "in accordance with the law", that it was therefore not necessary to examine if the interference had been necessary in a democratic society, and that accordingly there had been a violation of Article 8.

Article 6

It was first noted by the Court that the central question in the present case was whether the proceedings as a whole were fair, and it was not the function of the Court to deal with errors of fact or law allegedly committed by a national court unless they may have infringed rights and freedoms protected by the Convention. While Article 6 guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence, including as in the present case, unlawfully obtained evidence. In contrast to previous similar case law, the fixing of the listening device and the recording of the applicant's conversation were

not specifically unlawful in that they were contrary to domestic criminal law, but rather due to the fact that there was no statutory authority for the interference with the applicant's right to respect for private life, and that therefore such interference was necessarily not "in accordance with the law".

The Court then noted that the recording of the applicant's conversation was the only evidence, and the fact that the applicant had pleaded guilty was due to the decision by the judge that the evidence should be admitted. Again referencing previous similar case law, the Court recognised that the applicant had had ample opportunity to challenge both the authenticity and the use of the recording, and that at each level of jurisdiction the domestic courts had assessed the effect of the admission of the evidence on the fairness of the trial. The Court held that the domestic courts had had the discretion and the opportunity to exclude the evidence, if its admission could have given rise to substantive unfairness. Given the domestic courts' evaluation of the fairness of admitting the evidence, the Court therefore found that the use of the recording did not conflict with the right to a fair trial guaranteed by Article 6 § 1, and that accordingly there was no violation of Article 6.

Article 13

The Court first acknowledged that the courts in the criminal proceedings were not capable of providing a remedy, as it was not their purpose to deal with the substance of the Convention complaint that the interference with the right to respect for the applicant's private life was not "in accordance with the law". The Court agreed with the applicant's argument that the domestic law was not capable of affording a practical and effective remedy as required by Article 13, and referred to a previous finding of the Commission of a breach of Article 13 in similar circumstances. After an examination of the other avenues open to the applicant in respect of the Article 8 complaint, the Court found that the system of investigation of complaints did not meet the required standard of independence to meet the threshold of sufficient protection against the abuse of authority and thus provide an effective remedy within the meaning of Article 13. Accordingly, there had been a violation of Article 13.

Article 41

The Court considered that the finding of a violation under Article 8 constituted in itself sufficient just satisfaction for any damage which the applicant may have suffered, and made an award of £11,500 in respect of costs and expenses.

While those impacted by the existence of secret surveillance powers against citizens were "victims" for the purposes of admissibility, such measures did not violate Article 6, 8, or 13 of the Convention, as the provision of adequate safeguards against abuse, and the necessity for the protection of national security, made such measures both lawful and proportionate

JUDGMENT IN THE CASE OF
KLASS AND OTHERS v. GERMANY

(Application no. 5029/71)
6 September 1978

1. Principal facts

The applicants, German nationals, were lawyers and judges. In June 1971, the applicants alleged before the European Commission on Human Rights[270] (the Commission) that Article 10 para. 2 of the Grundgesetz ("Basic Law") and the Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post- under Fernmeldegeheimnisses, "G 10") empowered authorities to monitor the applicants' private correspondence without notice, thereby excluding the possibility of challenging such measures, in violation of their rights under Articles 6, 8, and 13 of the Convention.

While not directly targeted by State surveillance, the applicants stressed that they could nevertheless have been subject to invasions of their private correspondence, in the case that their clients could have been subject to surveillance without the applicants' knowledge. The Government did not contest that the applicants had been subjected to surveillance directed at another party.

The Commission found the applicants' arguments admissible, clarifying that, while the applicants may not themselves have been directly subject to the alleged violation, they should still be considered "victims" of the behaviour and be granted standing before the Court. Persons subject to secret measures by the authorities were not always subsequently informed of the measures taken against them. In consideration of this fact, the Commission found that, while it was not always

[270] From 1954-1998 the European Commission of Human Rights (Commission) acted as an intermediary between individual applicants and the European Court of Human Rights. Upon the passage of Protocol 11, the Commission was abolished, in favour of direct access to the Court.

possible for the applicants to demonstrate that their rights had been violated, they should nevertheless be entitled to lodge an application.

2. Decision of the Court

All applicants complained that two German laws regulating the surveillance of private communications, the "Basic Law" and the "G 10", ran contrary to their Article 6, 8, and 13 rights. Specifically, the applicants complained that these legislative provisions permitted the authorities to perform surveillance without the knowledge of those affected, and without clear requirements to notify those targeted upon terminating surveillance, in effect excluding remedy before the courts.

Article 25 (now Article 34)

The Court began by reviewing the status of the applicants as "victims" within the meaning of Article 25, and its impact on admissibility before the Court. Revisiting the Commission's determination regarding the applicant's victimhood, the Court reiterated that Article 25 did not permit an applicant to argue in abstracto that a State law or action contravenes the Convention.

The Court underlined, however, that Article 25 was foundational to the Convention's enforcement machinery and dependent upon individual access to the Commission. It was further highlighted that secret surveillance, which remains unknown and therefore unchallenged, could have the effect of reducing Article 8 to a nullity. The Court stressed that it was unacceptable that an individual may be deprived of their rights without remedy simply due to lack of awareness. In light of this principle, the Court accepted that an individual may rightfully claim to be the victim of a violation on the basis of the mere existence of legislation permitting secret measures against him.

The Court held that it had jurisdiction to rule on whether the applicants could claim to be victims within the meaning of Article 25, and that they could here make such a claim.

Article 8

The Court conceded that telephone conversations are entitled to Article 8 protections as a general matter, and that the existence of legislation permitting

secret surveillance, without adequate safeguards, was a potential menace to these protections. State surveillance powers, the Court emphasised, were tolerable only as strictly necessary for safeguarding democratic institutions.

All parties conceded the legitimacy of the Government's aims, namely, to safeguard national security, protect the rights of others, and deter crime. The Court highlighted that effective deterrence of newly emerging contemporary threats, such as technical advances in espionage and the rise of terrorism, sometimes required secret surveillance. Nevertheless, the Court highlighted that such measures threatened to undermine democracy whilst claiming to defend it, and that adequate safeguards against abuse were therefore essential.

As the nature of secret measures threatened to deprive individuals of the right to seek effective remedies of their own accord, the Court determined that it was critical that established procedures should themselves adequately protect individual rights. The Court paid particular attention to the extent to which the legislation in question provided and delineated such safeguards, including sufficient definition of the circumstances under which surveillance could be initiated, the restrictions on its scope and duration, limitations on the parties who could authorise surveillance, the existence of established reporting mechanisms for monitoring the progress and scope of surveillance, efforts to notify subjects of surveillance upon its cessation, available remedies for those who feel they have been wrongfully targeted or treated, and procedures for terminating surveillance found to be excessive or beyond the scope of the law.

Finding such safeguards to be in place, it remained to be determined whether existing standards were restrictive enough to limit surveillance measures to those strictly necessary to a democratic society. In the context of the applicants' case, this required striking an appropriate balance between the individual's Article 8 rights, and the necessity to impose secret surveillance for the protection of democratic society as a whole.

In the Court's view, this balance was not necessarily jeopardised merely by lack of notice. While the applicants asserted that lack of effective controls after the termination of surveillance served to make Article 8 rights illusory, the Court focussed on the extent to which such measures relied upon secrecy in order to achieve their legitimate ends. In as much as the interference with the applicants' rights was in accordance with the law and proportional to the legitimate aims pursued, the lack of notice to the individual could not itself be incompatible,

as secrecy was essential to the efficacy of the "interference". Nevertheless, the Court stated that the person impacted must be notified upon termination of the surveillance, as soon as doing so would not jeopardise the State's legitimate ends.

Finding that secret surveillance measures were sometimes necessary in a democratic society in the interests of national security and for the prevention of disorder, and finding that the legislation in question had established adequate safeguards and remedies to avoid the abuse of discretion, the Court held that there had been no violation of Article 8.

Article 13

Consistent with its conclusions that secret surveillance may sometimes be necessary in modern society in the interests of national security and for the prevention of disorder or crime, the Court concluded that the circumstances of the applicants' case did not entail a breach of Article 13.

The Court further found that the domestic remedies available to the applicants under German law, though limited in effectiveness, were as effective as could be expected or desired given the circumstances.

The Court unanimously held that there had been no violation of Article 13.

Article 6

In light of its conclusion that the Government's surveillance did not violate Article 8, in its examination of Article 6 the Court found it necessary to distinguish between the stages before and after notification of the termination of surveillance. In either case, the Court emphasised that the applicants had at their disposal several legal remedies against the possible infringements of their rights, and that these remedies would serve to satisfy the requirements of Article 6.

The Court accordingly concluded that Article 6 had not been violated.

Systematic publishing of tax debtors' personal data, including home address, was found to breach Article 8 of the Convention

GRAND CHAMBER JUDGMENT IN THE CASE OF

L.B. v. HUNGARY

(Application no. 36345/16)

9 March 2023

1. Principal facts

The applicant was born in 1966 and lived in Budapest.

Since 1996, under the Hungarian tax administration system, the National Tax and Customs Authority ("the Tax Authority") was required to publish data normally subject to taxpayer confidentiality in exceptional situations where this was in the public interest. This included where private individual taxpayers had accrued significant tax arrears exceeding HUF 10 million (approximately €28,000), or HUF 100 million in the case of legal entities (approximately €280,000).

In accordance with s55(3) of the Tax Administration Act 2003 ("the 2003 Act"), the Tax Authority was required to publish a list of major tax defaulters with data fields including the taxpayer's name, home address, commercial premises, tax identification number, in addition to the amount of the arrears. Where a final decision had been rendered establishing arrears from the previous quarter, the provision also required publication of the legal consequences where payment obligations ordered had not been met within the prescribed time period.

Following this, Act no. LXI of 2006 ("the 2006 Amending Act") added an additional subsection (5) to s55 of the Tax Administration Act, requiring that lists of major tax debtors be published, with data fields including the tax debtor's name (company name) and home address (registered office) where tax debts were in excess of HUF 10 million for a period longer than 180 days.

On 3 July 2013, following a tax inspection carried out earlier that year, the Tax Authority found that the applicant had a tax significant deficit, reduced by the second-instance Tax Authority following appeal to HUF 227,985,686 (approximately €625,000), classified as tax arrears.

The applicant had sought judicial review, however his action was dismissed by the Budapest Surroundings Administrative and Labour Court, as the applicant was found to have had issued fictitious invoices for a limited liability company at a point at which he no longer had a material relationship with it. Payment for the fictitious invoices was made into the company's bank account, from which the applicant withdrew HUF 715,025,000, paying no income tax on the sum. Notably, the company had neither the personnel nor material resources necessary to carry out any meaningful activity.

Subsequently, the applicant lodged a petition for review with the *Kúria* which upheld the first instance judgment, endorsing the reasoning of both lower decisions. Finally, the applicant lodged a constitutional complaint which was declared inadmissible.

The Tax Authority published the applicant's personal data, including name and home address, within the list of major tax defaulters on its website in the last quarter of 2014, pursuant to s55(3) of the 2003 Act. Subsequently, the applicant's name and home address were published on the list of "major tax debtors" on the Tax Authority website, pursuant to s55(5) of the 2003 Act.

On 16 February 2016 an online media outlet published an interactive map entitled "the national map of tax debtors". Here, the applicant's home address was indicated by a red dot, alongside the addresses of other tax debtors. By clicking on the red dot, the applicant's personal information (name and home address) was revealed, rendering the data accessible to all readers.

On 5 July 2018, the applicant's personal data was removed from the list of major tax debtors when his arrears became time-barred.

2. Decision of the Court

The applicant complained that publication of his name and home address on the list of major tax debtors on the website of the Tax Authority had violated his right to respect of private life under Article 8 of the Convention, in breach of his right to protection of his personal data. In its judgment of 12 January 2021, the Chamber held that there had been no violation of Article 8. At the applicant's request, in accordance with Article 43 of the Convention, the case was referred to the Grand Chamber.

Admissibility

The Grand Chamber limited the scope of its examination of the applicant's complaint to the publication of his personal data included in the list of major tax debtors under s55(5) of the 2003 Tax Administration Act. Hence, it did not proceed to examine the complaint concerning third-party republication of his personal data within a "national map of tax debtors" by the online news portal, as this matter did not form part of the "application as it has been declared admissible" by the Chamber in its examination, consequently falling outside the scope of the case referred to the Grand Chamber. However, the Grand Chamber did not exclude the risk of republication featuring as an element of its overall assessment.

Article 8

The Court found that the publication of the applicant's personal data could be considered an interference with his right to respect for private life. Furthermore, the impugned measure was established in accordance with the law.

The applicant contested the assertion that the interference with his right to respect for private life had served a legitimate aim, submitting that the aim of disclosure was public shaming. The Court however found that the impugned measure pursued a legitimate aim in the interest of the economic well-being of the State by optimising tax revenue and securing tax collection. Such a measure targeting non-compliance sought to enhance efficiency of the tax system. It was accepted that the measure's objective was to improve tax discipline and that disclosure of major tax debtors' personal data could be expected to have a deterrent effect. Furthermore, the Court accepted that the measures promoted transparency and reliability in business relations by providing an insight into the fiscal situation of tax debtors, protecting "the rights and freedoms" of third parties.

Assessing whether the interference had been "necessary in a democratic society", the Court examined whether a correct balance had been struck between, on the one hand, the public interest in ensuring tax discipline, the economic well-being of the country and the interest of potential business partners through the access to specific State-held data of private individuals against, on the other hand, the interest of private individuals in protecting certain forms of data retained by the State for tax collection purposes.

The Court highlighted that the publication in issue was not the individual decision of the Tax Authority, rather, it fell within the scheme set up by the legislature of systematic publication of major tax debtors' personal data on the Tax Authority's website, where those debtors met the objective criteria set out in s55(5). This applied to all taxpayers who, at the end of each quarter, owed large amounts of tax for a period longer than 180 consecutive days, regardless of the facts of each case. Neither individual circumstances nor the existence of any subjective fault were taken into account. It was a general measure to tackle non-compliance with tax payment obligations.

Given this general context, the Court examined whether the statutory scheme remained within the State's margin of appreciation. A wide margin of appreciation was afforded to States when assessing the need to establish a scheme for the dissemination of personal data of taxpayers who do not meet their tax payment responsibilities as a method of ensuring the proper functioning of tax collection systems. In determining its limits, however, the Court must be satisfied that a proper balancing exercise of competing interests was conducted by the competent domestic authorities.

The Court underlined the significance of the general measure to its findings. In particular, the publication scheme under the 2003 Act did not require the Tax Authority to undertake a balancing exercise evaluating competing individual and public interests, or an individualised proportionality assessment. Although a general scheme was not problematic in itself, nor was the publication of taxpayer data, the instant case was distinguished given that the data published included home address. In order to establish whether the respondent State had acted within its margin of appreciation, the Court proceeded to examine the quality of the parliamentary review of the necessity of the interference, and whether an adequate weighing-up exercise of competing interests had been conducted by the legislature in passing the impugned measure.

The Court noted the objectives of the legislature in passing the 2006 amendment to the 2003 Act which introduced s55(5), considering the measure necessary in order to "whiten the economy" and reinforce the capacities of the tax and customs authorities. However, the preparatory works did not demonstrate any assessment of the adequacy or impact of the publication schemes that already existed upon taxpayer compliance. Nor did they demonstrate consideration of any potential complementary value of the s55(5) scheme beyond the foreseeable consequence of harm to reputation that might arise from being identified on the list as a major tax debtor.

Furthermore, whilst an explanatory report to the 2003 Act referred to taxpayers' right to privacy to justify strict rules on confidentiality, there was no evidence that the same consideration was given with regard to the publication scheme under s55(5) of the 2006 Amending Act, or of any potential misuse of the tax debtor's residential address by the general public.

Finally, it was not evident that the unrestricted potential reach of the medium of publication of sensitive data, via the internet on the Tax Authority's website, had been given due consideration.

Consequently, the Court concluded that Parliament did not appear to have considered the extent to which publication of these sensitive categories of tax debtors' personal data was necessary in order to achieve its declared purpose, pursuant to the economic well-being of the country. It had not been shown that the legislature had attempted to strike a fair balance between public and private interests, in pursuit of the proportionality of the interference. Despite the margin of appreciation, considering the systematic nature of the publication of sensitive data including home address, although the reasons of the Hungarian legislature for enacting s55(5) were found to be relevant, the Court was not satisfied that they were sufficient to demonstrate that the interference was "necessary in a democratic society". Article 8 of the Convention was found to have been violated.

Article 41

The Court considered that the finding of a violation was in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant. The Court awarded €20,000 for costs.

The admissibility and use of personal medical data, and its subsequent public availability, during divorce proceedings amounted to a violation of Article 8

JUDGMENT IN THE CASE OF
L.L. v. FRANCE

(Application no. 7508/02)
10 October 2007

1. Principal facts

The applicant was born in 1957 and lived in France. On 5 February 1996, the applicant's wife filed for divorce. In a judgment of 4 September 1998, the responsible tribunal granted the divorce on grounds of fault by the applicant alone.

The applicant appealed the decision, requesting that the divorce be granted on grounds of fault by both spouses. He also requested that the court exclude from the case file a document from his medical records that his wife had allegedly obtained without his consent and on which she had relied to show that he was an alcoholic. The document was an operation report, dated 2 April 1994, concerning a splenectomy which the applicant had undergone which had been sent in a letter from a digestive specialist surgeon to the applicant's general practitioner. In the letter, the doctor had referred to a bout of acute pancreatitis with a background of alcoholism and indicated that the consequences of the pancreatitis could only be brought under control if the subject gave up alcohol.

In a judgment of 21 February 2000, the Court of Appeal upheld the provisions of the judgment and cited, among other evidence, proof of the applicant's alcohol-induced violence towards the applicant's wife, testimony regarding the applicant's alcoholism and the applicant's medical documents that the applicant's wife had presented. However, the court maintained the applicant's rights of contact and visitation with his children, with which he was satisfied.

2. Decision of the Court

The applicant submitted that the production and use of his medical documents in court without his consent entailed an unjustified interference with the right to respect for his private life under Article 8 of the Convention.

Article 8

To find a violation of Article 8, the Court must determine 1) whether the State's actions amounted to an interference with the applicant's right to respect for their private life, 2) whether it was in accordance with the law, 3) if it served a legitimate aim, and 4) whether that interference was justified, i.e. proportional and necessary in a democratic society.

The data contained in the applicant's medical documents related to his private life as they contained personal, medical information. Medical data constitutes personal data as defined in the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Court of Appeal partly based its decision on the content of the medical data, citing aspects of the medical report in its opinion. Because divorce decisions are publicly available, the applicant's personal medical information was made public as a result of its admissibility in the divorce proceedings and reproduction in the opinion. The Court found that the admissibility and use by the judge of the medical data in evidence constituted an interference with the applicant's right to respect for his private life as secured by Article 8 § 1.

In divorce proceedings, domestic law stipulated that evidence of the complaints submitted was unrestricted and could be adduced by any means, unless it was shown that it had been obtained by duress or fraud or that reports drawn up at the request of a spouse had given rise to unlawful interference with private life or trespass on domestic premises. In this case, there was no evidence produced that indicated that the medical reports had been obtained through duress, fraud, unlawful means or trespass. As such, the Court found, and the parties agreed, that the interference was in "accordance with the law" within the meaning of Article 8 § 2.

The aim of the interference in this case served the legitimate aim of "protect[ing] the rights and freedoms of others", namely the spouse's right to produce evidence in order to succeed in her claims. As such, the Court found that the interference served a legitimate aim within the meaning of Article 8 § 2.

In order to ascertain whether the interference was "necessary in a democratic society", the Court considered whether the reasons adduced to justify it were relevant and sufficient and whether it was proportionate to the legitimate aim pursued. The Court reiterated that the protection of medical data is of fundamental

importance to a person's enjoyment of their right to respect for private life – domestic law must therefore provide adequate safeguards to protect against the disclosure of personal health data. The Court also noted that the present case concerned civil proceedings in the area of divorce, which by definition are proceedings during which information on the intimacy of private and family life may be revealed and where it is in fact part of a court's duty to interfere in the couple's private sphere in order to weigh up the conflicting interests and settle the dispute before it. However, any unavoidable interference in this connection should be limited as far as possible to that which is rendered strictly necessary by the specific features of the proceedings and by the facts of the case.

The Court found that the interference was not proportionate to the aim pursued and was therefore "unnecessary in a democratic society for the protection of the rights and freedoms of others" because the evidence was not decisive for the granting of the divorce, and used on an alternative and secondary basis to other testimonies. The Court felt that, if the evidence had been declared inadmissible, the judge would have reached the same decision given the primary evidence presented.

Domestic laws did not afford sufficient safeguards in respect of the use and publication of personal data relating to the private life of parties to proceedings of this nature, and there had been a violation of Article 8.

Article 41

The Court awarded no damages as there was no causal link between the violation observed and the alleged pecuniary damages, and the finding of a violation constituted sufficient just satisfaction for the non-pecuniary damages sustained.

In the absence of clear, accessible legal rules and standards restricting the scope of police powers, the secret interception of private correspondence for the purposes of detecting crime was not in accordance with the law and violated the Article 8 right to respect for private life

JUDGMENT IN THE CASE OF

MALONE v. THE UNITED KINGDOM

(Application no. 8691/79)

2 August 1984

1. Principal facts

The applicant was born in the United Kingdom in 1937. In 1977 he and his wife, antique dealers, were arrested and charged with mishandling of stolen goods. They were ultimately acquitted, by combination of lack of prosecutorial evidence and a hung jury.

Following his trial, the applicant complained that he had reason to believe that his correspondence and telephone calls had been intercepted by the police beginning around 1974 and had continued to be monitored after his acquittal. While the Government generally declined to directly respond to these allegations, during trial it became clear that the applicant's telephone had been "tapped" on at least one occasion, during which a private conversation was recorded by police. The Government acknowledged that on this occasion the applicant's phone call had been intercepted, pursuant to a warrant from the Secretary of State and for the purpose of detecting crime.

Details of law and practice relating to the interception of private communications were initially established in the Report of the Birkett Committee, appointed in 1957. The Committee found that, while the origins of the power of the Secretary of State to intercept private communications were obscure, they had been legitimately exercised for several centuries in the case of physical correspondence, as well as since the invention of the telephone.

A Government White Paper published in 1980 reaffirmed the findings of the Birkett Committee: that the Secretary of State could authorise the interception of private correspondence in order to detect serious crime or safeguard the security of the State. The White Paper elaborated that the offense must be grave, that

other detection methods must have been tried but failed, and that there must be sound reason to believe that interception would lead to arrest and conviction.

In 1969, the Post Office Act had established the Post Office as a public corporation, rather than a Department of State. The Act articulated the functions and duties of the Post Office relative to its change in status, including express statutory provisions around the interception of communications on the authority of a warrant of the Secretary of State. Section 80 of the Act, among others, detailed these provisions. Later, in 1981, the British Telecommunications Act divided the Post Office, responsible for mail, and British Telecommunications, responsible for telephones, into two departments, with no functional difference to the governance of interceptions.

In proceedings against the Government before the Vice-Chancellor, the applicant unsuccessfully sought a declaration that the surveillance to which he had been subjected had been conducted unlawfully, in violation of his Article 8 rights. He contended that interceptions were more frequent than reported and utilised for reasons described in neither the Birkett Report nor the White Paper. The Vice-Chancellor found that there was no general right to privacy in English law, that telephone surveillance was not expressly forbidden, and that the Article 8 "Klass Case"[271] requirements were not satisfied in the applicant's case; he recommended legislation to address the lack of safeguards of private telecommunications, a recommendation that the Government declined to adopt. Based on these outcomes, the applicant argued he had exhausted all available domestic remedies, and brought his case before the Commission[272], who advanced the case to the Court.

2. Decision of the Court

The applicant complained that he was subject to unjustifiable secret surveillance on the part of the Government, in violation of his Article 8 right to respect for private life. The applicant further complained that the nature of secret surveillance generally was such that a victim may be effectively denied access to

[271] *Klass and Others v. Germany*, judgment of 8 September 1978, no. 5029/71, also included as a summary in this publication.

[272] From 1954-1998 the European Commission of Human Rights (Commission) acted as an intermediary between individual applicants and the European Court of Human Rights. Upon the passage of Protocol 11, the Commission was abolished, in favour of direct access to the Court.

an effective remedy in violation of Article 13, as the victim may never know that the surveillance had occurred, whether it had followed appropriate safeguards or procedures, and may never have access to the evidence required to take legal action against the State.

Article 8

The Court began by narrowing the scope of the case before it, emphasising that the discussion was to focus on the interception of private communications for the purposes of a police investigation only, not the broader question of Government surveillance of citizens in other contexts.

The Court referred to the Commission's prior analysis, which had established that the interception of postal and telephone communications, in order to detect a crime, constituted an interference with the applicant's Article 8 rights. The question was whether such an interference was justified, in accordance with the law, and necessary in a democratic society for the purpose of deterring crime. In particular, the applicant's complaints raised the questions of whether procedures regulating interception of private correspondence could be in accordance with the law if not directly regulated by law, and, relatedly, if such procedures offered adequate safeguards.

The Court stressed that, in order to be compatible with the rule of law, foreseeability serves as a necessary legal protection against arbitrary interference in a democratic society. A law must be sufficiently accessible so as to allow an individual to alter their behaviour in adherence. The Court further highlighted that legal regulations must clearly indicate the scope of power granted to the relevant authority, in order to adequately prevent abuse. The question, therefore, was whether the scope of powers in the case of interception of private communications was sufficiently accessible, foreseeable, limited and defined.

While the Government contended that Section 80 of the Post Office Act of 1969 defined and restricted the police power of interception, referencing time restrictions and limitations on the manner and recipient of intercepted information, the Court did not accept this argument. The Court instead highlighted that it was unclear which aspects of interception remained under the absolute discretion of the Secretary of State, and that there was a noticeable absence of clear restrictions on "purposes" or "manner" of interception. In particular, the Court referenced both the definition of "a serious crime," which had been expanded over time, as

well as internal disagreement on the part of the Government as to the degree to which Section 80 acted as a binding legal restriction.

The Court acknowledged that some degree of power to intercept communications, for the purpose of deterring or detecting crime, may be necessary in a democratic society within the meaning of paragraph 2 of Article 8, in particular in modern society. However, in order to be not only necessary to, but consistent with, democratic society, such interference could only be regarded as necessary if the system adopted retained adequate safeguards against abuse. One such safeguard being foreseeability, the Court noted that while laws must give citizens adequate notice of the circumstances under which secret surveillance may be utilised, they need not be so detailed as to allow individuals to adapt criminal behaviour in order to escape detection.

The Court then discussed the use of "metering" as distinct from other forms of government interference into private communications. It did not accept the Government's argument that, while distinguishable from the clear Article 8 concerns raised by other forms of surveillance, metering could never give rise to an Article 8 violation.

The Court held that the minimum level of clarity required to protect citizens from arbitrary government interference was lacking in the case of both traditional forms of interception and in metering, and that the interceptions therefore could not be found to be "in accordance with the law." In view of this holding, the Court did not find it necessary to consider further whether the Government's practices were "necessary to a democratic society."

Article 13

The Court held that it was not necessary to examine the case under Article 13.

Article 50 (now Article 41)

The Court held that Article 50 was not yet ready for an opinion and referred the question back to the Chamber. The applicant and Government subsequently reached a settlement agreement.

An order by the Greek public prosecutor to publish in a public announcement a photograph of the applicant and the details of the criminal charges against her, constituted a violation of Article 8

JUDGMENT IN THE CASE OF
MARGARI v. GREECE

(Application no. 36705/16)
20 June 2023

1. Principal facts

The applicant was born in 1978 and lived in Athens. On 16 November 2015, she was arrested along with six other persons, and charged with aiding and abetting fraud, forgery and use of forged documents, and participation in a criminal organisation, in order to commit fraud in relation to property transactions. The applicant and her co-accused were accused of obtaining more than €70,000 by impersonating estate agents and using forged documents to approach property owners and prospective buyers, and had then transferred or promised to transfer ownership of certain properties in order to fraudulently receive and steal deposits. On 25 November 2015, the Department of Public Security of the Eastern Attica Police asked the public prosecutor of the Athens Court of First Instance to publish the personal data and photographs of the accused. The public prosecutor then issued an order which authorised the publication of the data and photographs by any media outlets for a period of six months from 2 December 2015 to 2 June 2016. The order was approved by the public prosecutor of the Athens Court of Appeal, who considered that all the legal conditions for the order had been met. The order mentioned the applicant's name in fourth place, and the offences with which each individual was charged were distinguished from the charges against the other accused persons. A police announcement was then published on 16 December 2015 on the website of the Hellenic Police, which referred to "members of a criminal organisation that committed fraud at the expense of property owners", and listed the various charges against the accused. The applicant was the third person mentioned in the announcement, which did not distinguish between the charges made against the applicant and her co-accused.

On 26 December 2015 the applicant was informed of the publication of her personal data in various media outlets and websites by her friends rather than through any notification from the authorities. On 22 June 2017, the applicant was

convicted and sentenced to eleven years and six months' imprisonment without suspensive effect. The applicant and her co-accused appealed, but the applicant did not appear before the appellate court and was not represented. Her appeal was rejected as undefended, and the applicant was at the time of the European Court's judgment considered a fugitive.

2. Decision of the Court

The applicant complained that the publication of her photograph and personal data in the press for a period of six months following her being charged had violated her right to respect for private life as provided for in Article 8 of the Convention, and that she had had no effective remedy under Article 13.

Preliminary Issue

The Court first noted that although it was in doubt whether the applicant still wished to pursue the application, it had discretion under Article 37 to continue its examination "if respect for human rights as defined in the Convention and the Protocols thereto so requires". Considering that the publication of personal data by prosecuting authorities in the context of pending criminal proceedings was an especially significant human rights issue, the Court decided to continue the examination of the application on its merits.

Article 8

The applicant argued that the publication of her photograph and personal data, without her having prior knowledge of the publication, without her being able to contest the decision, and without her being distinguished from her co-accused as regards the offences she had been charged with, had given rise to a violation of Article 8. It was uncontested between the parties that there had been an interference with the applicant's right to respect for her private life, and the Court therefore turned to consider whether the interference was justified. It found that the interference was in accordance with the law, citing the provision of Greek law which permitted the public prosecutor to order the publication of personal data. The Court then considered whether the publication pursued a legitimate aim, and determined that the publication of the photograph and the data had pursued the legitimate aim of protecting the rights of freedoms of others in society, citing the order's justification that the publication aided the criminal investigation of other possible offences which the applicant and their co-accused might have committed.

The Court then turned to examine whether the publication was necessary in a democratic society. It highlighted the requirement of proportionality, and recognised that national authorities should be allowed to strike a fair balance between the conflicting public and private interests of publishing such information. Considering the photograph and the data separately, the Court noted that the objective usefulness of publishing the photograph derived from the fact that the applicant was not in custody, and the authorities could use the photograph in order legitimately enlist public support and investigate any other offences that might have been committed by the applicant and her co-accused. Regarding the data, the Court noted that only the necessary information to achieve the legitimate aim had been published, and that there was no statement contained in the order that would breach the presumption of innocence.

The Court then assessed the proportionality of the announcement, and took issue with the provision of Greek domestic law which allowed a derogation from the two safeguards (the right to appeal and the right to be notified in advance of publication) for certain offences. As the applicant had been charged with one of these offences, namely joining a criminal organisation, the police were able to publish the announcement without notifying the applicant, and without the possibility of appeal. Being the subject of criminal proceedings did not detract from the broader protection of an individual's private life, and the applicant should have been notified in advance of publication. Furthermore, the absence of a mechanism for the applicant to appeal against the prosecutor's order for the publication of her photograph and personal data meant that the process was not fair, and did not afford sufficient respect to the individual rights protected by the Convention. The Court emphasised that even though Article 8 of the Convention contained no explicit procedural requirements, it was important for the effective enjoyment of the rights guaranteed by the provision that the relevant decision-making process was fair and such as to afford due respect to the interests safeguarded by it.

Finally, the Court drew attention to the difference between the information contained in the order and that published in the announcement, highlighting that the order described in detail the exact charges each of the accused would face, while the announcement did not make any distinction between the applicant and the accused. As the announcement, and not the order, was published in the media, the Court held that the data therefore did not accurately reflect the situation and the charges against the applicant, amounting to a disproportionate interference in the applicant's right to respect for her private life. Therefore, the Court found that there had been a violation of Article 8.

Article 13

In light of its findings under Article 8, the Court considered that it was not necessary to separately examine the complaint under Article 13.

Article 41

The Court held that its finding of a violation of Article 8 constituted sufficient just satisfaction, and made no award.

Violation of Article 8 held where State secret surveillance of mobile telephone communications did not have a legal framework that provided for adequate and effective guarantees against arbitrariness and abuse

GRAND CHAMBER JUDGMENT IN THE CASE OF
ROMAN ZAKHAROV v. RUSSIA

(Application no. 47143/06)
4 December 2015

1. Principal facts

The applicant, Roman Zakharov, was a Russian national, born in 1977, and the editor-in-chief of a publishing company. He subscribed to the services of several mobile network operators.

In December 2003 he brought judicial proceedings against three mobile network operators, complaining about an interference with his right to privacy of his telephone communications. He maintained that, under the relevant national law – specifically pursuant to Order no. 70 issued by the Ministry of Communications – the mobile operators had installed equipment that allowed unrestricted interception of all telephone communications by the security services without prior judicial authorisation. He asked the District Court in charge to remove the equipment installed under Order no. 70, which had never been published, and to ensure that access to telecommunications was given to authorised persons only. In December 2005 the District Court of St Petersburg dismissed the applicant's claims, finding that the installation of the equipment did not in itself infringe the privacy of his communications, and that the applicant had failed to prove that his telephone conversations had been intercepted.

The applicant appealed. He claimed that the District Court had refused to accept several documents in evidence, including judicial orders authorising the interception of several people's mobile telephone communications, which, in the applicant's opinion, proved that the mobile network operators and law-enforcement agencies were technically capable of intercepting all telephone communications without obtaining prior judicial authorisation. In April 2006 the St Petersburg City Court upheld the judgment on appeal, confirming the District Court's decision.

2. Decision of the Court

Relying on Article 8 of the European Convention on Human Rights, the applicant complained about the system of covert interception of mobile telephone communications in Russia, arguing that the relevant national law permitted the security services to intercept any person's communications without obtaining prior judicial authorisation. Relying on Article 13, he further complained he had no effective legal remedy at national level to challenge that legislation.

Article 8

The Court observed that, although the Convention does not provide for the institution of an actio popularis, Mr Zakharov was entitled to claim to be a victim of a violation of the Convention, even though he claimed that there had been an interference with his rights as a result of the mere existence of legislation permitting secret surveillance measures, and was unable to allege that he had been the subject of a concrete measure of surveillance. Given the secret nature of the surveillance measures provided for by the legislation, their broad scope – affecting all users of mobile telephone communications – and the lack of effective means to challenge them at national level, the Court considered an examination of the relevant legislation in abstracto to be justified. In view of the above, the Court considered that the applicant did not need to demonstrate that he was at risk of having his communications intercepted, as the mere existence of the contested legislation amounted in itself to an interference with his rights under Article 8.

Once determined that interception of mobile telephone communications had a basis in Russian law – namely the Operational-Search Activities Act (OSAA), the Code of Criminal Procedure (CCrP), and Order no. 70 issued by the Ministry of Communications – which pursued the legitimate aim of the protection of national security and public safety, the Court had to ascertain whether that domestic law was accessible and contained adequate and effective safeguards and guarantees.

Accessibility of domestic law

The Court found regrettable that the addendums to Order no. 70 had never been published in a generally accessible official publication. However, considering that it had been published in an official ministerial magazine, and that it could be accessed by the general public through a privately-maintained Internet legal

database, the Court did not find it necessary to pursue further the issue of the accessibility of domestic law.

Scope of application of secret surveillance measures

The Court considered that Russian legislation sufficiently clarified the nature of the offences which might give rise to an interception order. At the same time it noted with concern that the law lacked clarity concerning some of the categories of people liable to have their telephones intercepted, namely a person who could have information about an offence, or relevant to a criminal case, or those involved in activities endangering Russia's national, military, economic or ecological security. To that regard, the OSAA gave the authorities an almost unlimited degree of discretion in determining what constituted such a threat, and whether that threat was serious enough to justify secret surveillance.

The duration of secret surveillance measures

Russian law contained clear rules on the duration and renewal of interceptions providing adequate safeguards against abuse. Nevertheless, the Court noted that the requirement to discontinue interception when no longer necessary was mentioned in the CCrP only, and not in the OSAA. It followed that interceptions in the framework of criminal proceedings had more safeguards than those in connection with activities endangering Russia's national, military, economic or ecological security.

Procedures for storing, using, communicating and destroying the intercepted data

The Court was satisfied that Russian law contained clear rules governing the storage, use and communication of intercepted data, making it possible to minimise the risk of unauthorised access or disclosure.

As regards the destruction of such material, the Court found that Russian law was not sufficiently clear, as it permitted automatic storage for six months of irrelevant data in cases where the person concerned had not been charged with a criminal offence, and in cases where the person had been charged with a criminal offence it was not clear as to the circumstances in which the intercept material would be stored and destroyed after the end of the trial.

Authorisation of interceptions

The Court noted that Russian law contained an important safeguard against arbitrary or indiscriminate secret surveillance, dictating that any interception had to be authorised by a court. The law-enforcement agency seeking authorisation for interception had to submit a reasoned request to that effect to a judge, and the judge had to give reasons for the decision authorising interception.

As regards the scope of the review, judicial scrutiny was limited, and despite the recommendations of the Constitutional Court, judges did not verify the existence of a "reasonable suspicion" against the person for whom interception had been requested or examine whether interception was necessary and justified. As a result, interception requests were often not accompanied by any supporting materials, judges never requested the interception agency to submit such materials, and a mere reference to the existence of information about criminal offences or activities endangering national, military, economic or ecological security was considered to be sufficient for the authorisation to be granted.

With respect to the content of the interception authorisation, the Court observed that, unlike the CCrP, the OOSA granted a very wide discretion to the law enforcement authorities. The OOSA did not contain requirements neither with regard to the content of the request for interception nor to the content of the interception authorisation, meaning that courts sometimes granted interception authorisations which did not mention a specific person or telephone number to be tapped, but authorised interception of all telephone communications in the area where a criminal offence had allegedly been committed, and on occasions without mentioning the duration for which interception was authorised. Moreover, the non-judicial "urgent procedure" provided by the OOSA – under which it was possible to intercept communications without prior judicial authorisation for up to forty-eight hours – lacked sufficient safeguards to ensure that it was used only in duly justified cases. The authorisation procedures provided for by Russian law were not capable of ensuring that secret surveillance measures were not ordered haphazardly, irregularly or without due and proper consideration.

Furthermore, the Court considered that a system, such as the Russian one, which enabled the secret services and the police to intercept directly the communications of each and every citizen without requiring an interception authorisation to the communications service provider was particularly prone to abuse. The need for safeguards against arbitrariness appeared therefore to be particularly great.

Supervision of the implementation of secret surveillance measures

The Court examined whether supervision of interception complied with the requirements under the Convention that supervisory bodies be independent, open to public scrutiny and vested with sufficient powers and competence to exercise effective and continuous control.

Firstly, the Court noted the that prohibition on logging or recording interceptions set out in Russian law made it impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. Combined with the law-enforcement authorities' technical ability to intercept directly all communications, this law rendered any supervision arrangements incapable of detecting unlawful interceptions, and therefore ineffective.

Secondly, supervision of interceptions carried out on the basis of proper judicial authorisations was entrusted to the President, Parliament, and the Government, who were given no indication under Russian law as to how they could supervise interceptions, as well as the competent prosecutors, whose manner of appointment and blending of functions, with the same prosecutor's office giving approval to requests for interceptions and then supervising their implementation, could raise doubts as to their independence. Furthermore, the prosecutors' powers and competences were very limited, supervision conducted by them was not open to public scrutiny, and their brief semi-annual reports on operational search measures were confidential documents, not published or otherwise accessible to the public.

Lastly, the Court considered that the prosecutors' supervision of interceptions was not capable of providing adequate and effective guarantees against abuse. To that regard, the applicant had submitted documents illustrating prosecutors' inability to obtain access to classified materials on interception, whereas the Government had not submitted any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach in law.

Notification of interception of communications and available remedies

The issue of notification of interception of communications was inextricably linked to the effectiveness of remedies before the courts. The Court observed that in Russia persons whose communications had been intercepted were not notified of this fact at any point – unless that information became known as a result of

its use in evidence in eventual criminal proceedings – and that the possibility to obtain information about interceptions was particularly ineffective.

A remedy was available only to persons who were in possession of information about the interception of their communications. The effectiveness of the remedy in question was therefore undermined by the absence of a requirement to notify the subject of interception, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, Russian law did not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject. Also, Russian law did not provide for effective remedies to a person who suspected that he or she had been subjected to secret surveillance. By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschewed an important safeguard against the improper use of secret surveillance measures.

Conclusion

The Court concluded that Russian legal provisions governing interceptions of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. The shortcomings in the legal framework as identified by the Court indicated the existence of arbitrary and abusive surveillance practices, hence the Russian law did not meet the "quality of law" requirement and was incapable of keeping the interception of communications to what was "necessary in a democratic society". There had accordingly been a violation of Article 8 of the Convention.

Article 13

Having regard to the findings under Article 8 it was not necessary to examine the complaint under Article 13 separately.

Article 41

The Court ruled that the finding of a violation constituted in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant. It further held that Russia was to pay him the sum of €40,000 in respect of costs and expenses.

Retention of fingerprints and DNA profiles by the authorities constituted a violation of Article 8

GRAND CHAMBER JUDGMENT IN THE CASE OF

S. AND MARPER v. THE UNITED KINGDOM

(Application nos. 30562/04 and 30566/04)

4 December 2008

1. Principal facts

The applicants, S. and Michael Marper, were born in 1989 and 1963 respectively and lived in the United Kingdom.

On 19 January 2001 the first applicant was arrested and charged with attempted robbery, aged eleven at the time. His fingerprints and DNA samples were taken. He was acquitted on 14 June 2001. The second applicant was arrested on 13 March 2001 and charged with harassment of his partner. His fingerprints and DNA samples were taken. On 14 June 2001, the case was formally discontinued as he and his partner had become reconciled.

Once the proceedings had been terminated, both applicants unsuccessfully requested that their fingerprints, DNA samples and profiles be destroyed. The information had been stored on the basis of a law authorising its retention without any time limit.

2. Decision of the Court

The applicants complained under Articles 8 and 14 of the Convention about the retention by the authorities of their fingerprints, cellular samples and DNA profiles after their acquittal or discharge.

Article 8

The Court considered that the cellular samples and DNA profiles, as well as the fingerprints, contained sensitive personal information and that their retention amounted to an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 § 1 of the Convention. The Court also noted that the retention of the applicants' fingerprint, biological samples

and DNA profiles had a clear basis in the domestic law under the Police and Criminal Evidence Act 1984, and that it pursued a legitimate purpose, namely the detection, and therefore, prevention of crime.

The Court indicated that the domestic law had to afford appropriate safeguards to prevent any such use of personal data as could be inconsistent with the guarantees of Article 8. Further, the need for such safeguards was all the greater where the protection of personal data undergoing automatic processing was concerned, not least when such data were used for police purposes.

The issue to be considered by the Court in this case was whether the retention of the fingerprint and DNA data of the applicants, as persons who had been suspected, but not convicted, of certain criminal offences, was necessary in a democratic society.

The Court took due account of the core principles of the relevant instruments of the Council of Europe and the law and practice of the other Contracting States, according to which retention of data was to be proportionate in relation to the purpose of collection and limited in time.

The United Kingdom appeared at the time to be the only jurisdiction within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence. The data in question could be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; the retention was not time-limited; and there existed only limited possibilities for an acquitted individual to have the data removed from the nationwide database or to have the materials destroyed.

The Court expressed a particular concern at the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who had not been convicted of any offence and were entitled to the presumption of innocence, were treated in the same way as convicted persons. The retention of unconvicted persons' data could be especially harmful in the case of minors such as the first applicant, given their special situation and the importance of their development and integration in society.

In conclusion, the Court found that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of

persons suspected but not convicted of offences, as applied in the case of the present applicants, failed to strike a fair balance between the competing public and private interests, and that the respondent State had overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention in question constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society. The Court concluded that there had been a violation of Article 8 in this case.

Article 14 in conjunction with Article 8

In the light of the reasoning that led to its conclusion under Article 8 above, it was not necessary to examine separately the complaint under Article 14.

Article 41

The Court considered that the finding of a violation, with the consequences that this would have for the future, could be regarded as constituting sufficient just satisfaction in respect of the non-pecuniary damage sustained by the applicants. The Court awarded the applicants €42,000 in respect of costs and expenses, less the amount already paid to them in legal aid.

Article 46

The Court noted that, in accordance with Article 46 of the Convention, it would be for the respondent State to implement, under the supervision of the Committee of Ministers, appropriate general and/or individual measures to fulfil its obligations to secure the right of the applicants and other persons in their position to respect for their private life.

The use of an unlawfully obtained recording of a telephone conversation in the conviction of the applicant for attempted incitement to murder did not violate Article 6

JUDGMENT IN THE CASE OF
SCHENK v. SWITZERLAND

(Application no. 10862/84)
12 July 1988

1. Principal facts

The applicant was born in 1912 and lived in Tartegnin, Switzerland. In 1947, he married Josette P ("Mrs Schenk"), who was born in 1927. In 1974, the applicant filed a petition for divorce, which was granted on 10 December 1981. Earlier that year, on 28 February 1981 the applicant went to an advertising agency, where under an assumed name he gave instructions for an advertisement to be published: "*Wanted. Former member of the Foreign Legion or similar for occasional assignments; offer with telephone number, address and curriculum vitae to RTZ 81 poste restante CH Basle 2.*" The applicant selected Mr Richard Pauty, whom he met on several occasions and paid to carry out a variety of assignments, including one in Haiti in May 1981. Mr Pauty returned to Switzerland from Haiti on 12 June and telephoned Mrs Schenk on the 18 June. Mr Pauty visited Mrs Schenk on 19 June and told her that he had been commissioned by her husband to kill her. They then went together to the investigating judge of the Canton of Vaud on 20 June 1981. At the police station, the investigating judge interviewed Mr Pauty and Mrs Schenk. On 22 June, the investigating judge asked the French authorities to further an investigation into an attempted murder, and that one Inspector Messerli should be authorised to take part in them.

On 24 June, Mr. Pauty was interviewed in the presence of Inspector Messerli. Mr Pauty said, inter alia: "*RTZ 81, that is to say Mr. Pierre Schenk, will certainly contact me before long to ask for details of the murder of his wife, Josette Schenk. He is supposed to send me or bring me the agreed amount of $40,000. You asked me to come here and I would now ask you to give me instructions as to how I should act when Mr. Schenk contacts me.*" Mr Pauty was expecting the applicant to telephone him, and he set up a cassette recorder at his mother's home at Houilles near Paris and connected it by microphone to the second earphone of the telephone receiver. On the morning of 26 June, the applicant telephoned Mr Pauty from

a kiosk, and Mr Pauty recorded the conversation. At about 10am, Mr Pauty telephoned Inspector Messerli, played the recording back to the inspector, and asked him whether he would like to have the cassette. Inspector Messerli said that he would like to have the cassette, and approximately one hour later Mr Pauty arrived at the Crime Squad's offices and handed the cassette over to him. On 30 June 1981, Inspector Messerli played the recording to Mrs Schenk so that she could identify her husband's voice. The applicant was arrested the next day, and on 13 August 1982, was found guilty of attempted incitement to murder and sentenced to 10 years imprisonment by the Rolle Criminal Court. The applicant subsequently made appeals to the Criminal Cassation Division of the Vaud Cantonal Court and the Federal Court, both of which were dismissed, before lodging his application with the Commission[273] on 6 March 1984, which ruled that there had been no violation of the Convention.

2. Decision of the Court

The applicant complained that making a recording of his telephone conversation with Mr Pauty, and subsequently using it as evidence, was a violation of Article 6 § 1 of the Convention. The applicant also complained that owing to the use of the unlawfully obtained recording, he had not been proven guilty "according to law", and that there had been a failure to apply the principle of the presumption of innocence guaranteed in Article 6 § 2. Finally, the applicant complained under Article 8 that he was a victim of a violation of his right to respect for his private life and his correspondence, a right which included the right to confidentiality of telephone communications.

Article 6 § 1

The Government did not dispute that the recording of the telephone conversation between the applicant and Mr Pauty had been obtained unlawfully, although it was accepted that all three domestic courts had admitted the recording in evidence. As Article 6 does not lay down any rules on the admissibility of evidence, it was emphasised that the Court's role was to ascertain whether the applicant's trial as a whole was fair, and not to exclude unlawfully obtained evidence as a matter of principle and in the abstract. Unless a national court had

[273] From 1954-1998 the European Commission of Human Rights (Commission) acted as an intermediary between individual applicants and the European Court of Human Rights. Upon the passage of Protocol 11, the Commission was abolished, in favour of direct access to the Court.

infringed rights and freedoms protected by the Convention, the Court noted that it was not its function or its role to deal with errors of fact or of law allegedly committed by said national court.

It was then first noted by the Court that the rights of the defence had not been disregarded, and that the applicant had had opportunities to challenge the authenticity of the recording and to oppose its use as evidence against him. It was stated that the applicant had been aware that the recording had been obtained unlawfully, and in fact he had originally agreed that the recording should be heard in court. Furthermore, the applicant's counsel had not sought to examine Mr Pauty during the first trial, and the applicant had not summoned Inspector Messerli to appear. It was further noted that in any case it would have been sufficient to hear the evidence of Mr Pauty as a witness in respect of the recording's content, which was a further reason that the cassette had not been declared inadmissible. Finally, the Court noted that the recording was not the only evidence which the Rolle Criminal Court had relied on in the applicant's conviction, and that a combination of evidential elements had been taken into account, which were detailed in full across several passages of its judgment. Under these reasons, the Court found that the use of the unlawfully obtained recording of the conversation between the applicant and Mr Pauty did not deprive the former of a fair trial, and there had been no violation of Article 6 § 1.

Article 6 § 2

The applicant complained that owing to the use of the unlawfully obtained recording, he had not been proved guilty "according to law". In the applicant's submission there had been a failure to apply the principle of the presumption of innocence which was guaranteed in Article 6 § 2. The Court found that there was nothing to suggest that the Rolle Criminal Court had treated the applicant as if he were guilty before it convicted him, and the mere inclusion of the cassette and the recording in the evidence did not support the applicant's allegation of neglect of the presumption of innocence. Therefore, the Court found that there was no breach of Article 6 § 2.

Article 8

The applicant claimed lastly to be the victim of a violation of his Article 8 right to respect for his private life and his correspondence, which included the right to confidentiality of telephone communications.

The Court noted that the Commission had already declared the applicant's complaint inadmissible concerning the making of the recording under Article 8 in its decision of 6 March 1986, on the ground that domestic remedies had not been exhausted. Hence, the Court held that it had already dealt with the use made of the cassette during the judicial investigation and the trial from the point of view of Article 6, and that it was not necessary to examine the possibility of a violation of Article 8.

The transmission of data which had been lawfully obtained as part of a criminal investigation to the Dutch Competition Authority, and used in separate competition law proceedings, did not violate Article 8

JUDGMENT IN THE CASE OF
SHIPS WASTE OIL COLLECTOR B.V. v. THE NETHERLANDS[274]

(Application no. 2799/16)
16 May 2023

1. Principal facts

The applicant was a Dutch company involved in the collection of waste liquids from ships in the Rotterdam port region. In April 2008, as part of a criminal investigation into the potential illegal disposal of polluted waste, the Intelligence and Investigation Service of the Ministry of Housing, Spatial Planning and the Environment, operating under authorisation by an investigating judge, intercepted and recorded telephone conversations between an employee of one of the companies being investigated, and an employee of the applicant, which contained indications of price-fixing between them.

These recordings were judged to be of potential interest to the Netherlands Competition Authority ("the NMA"). In accordance with the Judicial and Criminal Data Act ("the WJSG"), the Public Prosecution Service ("the PPS") gave permission for the recordings to be transmitted to the NMA. The various recordings were transmitted on several occasions, beginning in June 2009 and continuing into 2010.

The NMA subsequently started an official investigation into possible violations of the Competition Act ("the Act"), which culminated in a finding of a violation by the applicant of section 6 of the Act. In November 2011, the NMA imposed a fine of €834,000 on the applicant. Along with several other Dutch companies which had also been found to have committed violations of section 6 of the Act, the applicant launched a successful appeal to the Regional Court, which quashed the NMA's decisions. After a further appeal by the successor body to the NMA to the

[274] Note that a request for referral to the Grand Chamber under Article 43 has been accepted, and the Grand Chamber will hand down a new judgment in this case.

Supreme Administrative Court for Trade and Industry, a judgment given in July 2015 quashed the Regional Court's judgment, dismissed the applicant company's cross-appeal and referred the case back to the Regional Court.

2. Decision of the Court

The applicant relied on Article 8 (right to respect for private and family life), and Article 13 (right to an effective remedy) of the Convention, complaining that the transmission and subsequent use of data that was irrelevant to the criminal investigation constituted a violation of its rights under Article 8, and that it had not had access to an effective remedy as provided for in Article 13.

Article 8

The Court assessed whether there had been a violation of Article 8 by examining: (i) whether there had been an interference, (ii) whether the interference was in accordance with the law, (iii) whether there was a legitimate aim for the interference, and (iv) whether the interference was necessary in a democratic society.

In respect of (i), the Court reiterated that legal persons may claim rights to respect of their business premises and correspondence under Article 8, and accepted that the transmission to the NMA of data obtained in the criminal investigation through tapping of telephone conversations had constituted an interference with the applicant's rights under Article 8.

In respect of (ii), the Court first emphasised that the applicant's complaints concerned the transmission of data which had been legally collected as part of a criminal investigation, and the subsequent use of this data in competition law proceedings. The applicant's complaints did not concern the interception of the data itself, the lawfulness of which was not disputed. The Court therefore proceeded on the basis that the data had been obtained through methods compatible with Article 8.

The Court recognised the fact that the transmission of data had occurred without the applicant's knowledge raised the issue of the law's foreseeability requirement in the context of secret surveillance. The applicant had argued that it had not been foreseeable that data which had no relevance to the criminal investigation would qualify as criminal data within the meaning of the WJSG,

and would therefore be transmissible. The applicant had also argued that the transmission had not been foreseeable as the legislation had failed to set out in sufficient detail the extent of the authorities' discretion to exercise their powers under the WJSG.

Referring to earlier case law, the Court drew attention to the requirement that the national law must be sufficiently foreseeable to enable individuals to act in accordance with it, and clarified that this foreseeability requirement, in the context of secret surveillance measures, could not mean that an individual should be able to foresee when the authorities would be likely to intercept communications. The Court held that as the data was intercepted and subsequently transmitted as part of two separate criminal investigations, the foreseeability requirement did not mean that the authorities had to notify the applicant that criminal data would be transmitted to the NMA. The Court found that the interference had a legal basis under section 39f of the WJSG, which set out the limits of, and the conditions for, the transmission of data by the PPS. The Court noted that section 39f made explicit provision for authorities charged with the enforcement of legislation as being authorised to receive criminal data, and further considered that it was clear that the NMA was charged with the enforcement of the Act. Therefore, the Court found that it was sufficiently foreseeable that the NMA was authorised to receive criminal data, and that the transmission of the data had been in accordance with the law.

In respect of (iii), the Court made reference to previous competition law cases, and accepted the Government's argument that it was evident that the data transmission had served the legitimate aim of protecting the economic well-being of the country.

In respect of (iv), the Court noted that section 39f of the WJSG had set out the limits and conditions for the transmission of criminal data by the PPS, which constituted sufficient safeguarding measures to prevent the abuse of interferences. The Court also noted that the WJSG's legislative history explicitly linked a "compelling general interest" to the legitimate aims listed in Article 8 § 2. After recognising the significance of the ex post facto judicial oversight procedure, and finding that the domestic courts had performed the required balancing act by adequately considering the competing interests of the applicant company, against the authorities' interests to protect the economic well-being of the country, the Court held that the interference had been necessary in a democratic society.

The Court hence found that the transmission of the data concerned was in compliance with Article 8, and that there had been no violation.

Article 13

The Court found that the applicant had not been deprived of an effective remedy due to not being notified of the transmission beforehand, and that following on from its examination of Article 8, the applicant had had avenues at its disposal to raise its complaints, and hence there had been no violation of Article 13.

Following unregulated searches and seizure of documents at company premises on the basis of an ordinance aimed at suppressing offences against economic laws, the concept of "home" was found to extend to professional premises, and a violation of Article 8 was found

CASE OF

SOCIÉTÉ COLAS EST AND OTHERS v. FRANCE

(Application no. 37971/97)
16 April 2002

1. Principal facts

The three applicant companies, located in different regions of France, engaged in public road works. Following complaints that large construction firms were partaking in certain illegal practices, the applicant companies became the subject of a large-scale investigation into the conduct of public-works contractors in local tendering procedures regarding 56 companies over 17 *départements,* conducted by the Department for Competition, Consumer Affairs and Fraud Prevention ("the DGCCRF").

On 19 November 1985, DGCCRF inspectors carried out simultaneous raids on fifty-six companies without authorisation from the companies' management, seizing several thousand documents. This was followed by further enquiries conducted on 15 October 1986, in order to gather statements. The inspectors entered the applicant companies' premises under the provisions of Ordinance no. 45-1484 of 30 June 1945 on the identification, prosecution and elimination of breaches of financial legislation, which enabled them to do so without any judicial authorisation or supervision.

During the raids, the inspectors seized various documents evidencing unlawful agreements pertaining to specific contracts which were not included of the list of contracts concerned by the investigation. On the basis of these documents, the Competition Council was asked both by the Minister of the Economy, Finance and Privatisation and the DGCCRF to investigate alleged illegal practices, following which the applicant companies received substantial fines.

The applicants contested the lawfulness of the searches and seizures carried out without judicial authorisation under the 1945 ordinance before the Paris

Court of Appeal which, following retrial, upheld the fines, although reduced them. Subsequent appeal to the Court of Cassation was rejected.

2. Decision of the Court

Relying on Article 8 of the Convention, the applicant companies complained that the raids carried out by official inspectors on both 19 November 1985 and 15 October 1986, conducted without any supervision or restriction, infringed their right to respect for their home.

Article 8

The Court began by restating the principles established under Article 8 of the Convention and their applicability to the "homes" of juristic persons, such as the applicant companies. Reiterating the status of the Convention as a living instrument, it was held that in certain circumstances, the rights guaranteed by Article 8 may be construed as including the right to respect for a company's registered office, branches or other business premises.

The Court found that the raids carried out at both principal and local offices of the applicant companies for the purposes of seizure, in order to obtain evidence of unlawful agreements between public-works contractors in the award of roadworks contracts, constituted an interference with the right of these companies to respect for their home. Furthermore, they were conducted in accordance with the law and in pursuit of legitimate aims for the purposes of Article 8 § 2, both in the interest of the country's economic well-being and the prevention of criminal offences.

However, turning to the question of whether the impugned interference might be considered "necessary in a democratic society", the Court noted that although such an interference might have been justified by the need for large-scale operations to avoid the disappearance or concealment of evidence of anti-competitive practices, the relevant legislation and practices should nonetheless have ensured adequate and effective safeguards against abuse. The Court found that this was not followed in the instant case. Under the 1945 order as it was then applicable, legislative reforms of 1986 not yet having effect, the relevant department had very broad powers that allowed it alone to determine the expediency, number, duration and scale of such operations. Furthermore, these operations had taken place without any prior warrant issued by a judge and in the absence of a senior police officer.

Consequently, although the Court accepted that the right to interfere might be more extensive in the case of a company's commercial premises, given the nature of the disputed searches and seizures conducted in the competition field, they could not be considered to be proportionate to their legitimate aims. Hence, a violation of Article 8 was found.

Article 41

The Court awarded each applicant €5,000 for damages and €6,700, €12,000 and €4,400 respectively to the applicant companies for costs and expenses.

The disclosure of an individual's identity, in a published judgment to which only the local authority and not the applicant were a party, and where they were accused of stigmatising behaviour, violated the right to respect for private life in Article 8

JUDGMENT IN THE CASE OF
VICENT DEL CAMPO v. SPAIN

(Application no. 25527/13)
6 November 2018

1. Principal facts

The applicant was born in 1957, and lived in León, Spain. He worked as a teacher and department head for the León School of Arts and Crafts, a local public school. Beginning in 2006, a colleague and teacher within his department filed several complaints against the applicant with local and regional authorities. The complaints accused the applicant of psychologically harassing the colleague at their workplace.

Upon having her complaints dismissed by local and regional authorities, the colleague instituted judicial proceedings against the educational administration for its failure to prevent the alleged harassment, unbeknownst to the applicant. In 2011, the High Court of Justice of Castilla-León judged that repeated psychological harassment had taken place, including routine public humiliation and death threats, identifying the applicant by name. The High Court of Justice ordered the administration to pay €14,500.

The applicant later learned of the judgment through a local newspaper report, at which time he requested to become a party to the proceedings. The High Court of Justice rejected his request, concluding that he could not be considered an "interested party" in a proceeding against the educational administration.

2. Decision of the Court

The applicant complained that the High Court of Justice had violated his rights under Article 8 of the Convention by publicly associating him with the stigmatic charge of harassment, adversely affecting his private and family life, reputation, and employment prospects. The applicant further complained that, by refusing his request to become a party to the proceedings, the High Court of Justice had

denied him his right of access to a court, and therefore his right to an effective remedy, in violation of Articles 6 and 13, respectively.

Article 8

The Court emphasised that the High Court of Justice had both the ability and the obligation to take appropriate measures to protect parties' reputations and private lives, including the discretion to withhold names within the judgment, to avoid identifying unidentified parties wherever possible, and to restrict publication or access to the judgment in order to protect named individuals.

The Court found that the actions of the High Court of Justice interfered with the applicant's Article 8 rights. When the High Court of Justice determined that the alleged actions constituted repeated psychological harassment and identified the applicant by name, it subjected him to stigma capable of significantly impacting his personal life. Such impacts included the potential loss of enjoyment of private and family life, relational or reputational damage, and harm to moral integrity and personal honour.

The High Court of Justice had operated in accordance with the law, and with the legitimate aims of judicial transparency, discouraging workplace harassment, and holding local authorities accountable for its prevention. However, the Court found that the High Court of Justice had declined to confine its reasoning to the immediate questions of whether the alleged treatment constituted harassment, and, if so, whether the educational authority was strictly liable for its failure to protect the colleague. Per relevant domestic law and practice, liability on the part of the educational authority was not contingent upon identifying the individual responsible for harassment; the decision to name the applicant was within the High Court of Justice's discretion. Barring further public policy justification, the intrusion into the applicant's Article 8 rights was therefore unwarranted.

Furthermore, once delivered the judgment would be made public, available to third parties and the media, and beyond the supervisory control of the High Court of Justice. In this instance, the case had significant repercussions in the media, as evidenced in part by the applicant's discovery of the proceedings via local newspaper reporting. Because the applicant was not a party to the proceedings, and was neither summoned over their course nor informed of their progression, the disclosure of the applicant's identity could not have been considered a foreseeable consequence of his own actions. The Court underlined

that, not having been made aware of the proceedings until after judgment had been rendered, the applicant was denied the opportunity to either defend himself or to request that his identity not be publicly disclosed.

Protective measures were readily available and could have significantly ameliorated damage to the applicant's private life. In addition, the High Court of Justice had an affirmative obligation to protect the parties' Article 8 rights to reputation. Taking all of this into consideration, the High Court of Justice's failure to introduce effective and available safeguards, without adequate justification, was disproportionate to the legitimate aims pursued.

The Court hence found that there had been a violation of the applicant's Article 8 right to respect for private life.

Article 6 § 1

Finding the applicant's arguments as it related to Article 6 § 1 to be linked to the denial of his Article 8 rights, it was not necessary to independently consider this claim.

Article 13

Further, finding the applicant's arguments as it related to Article 13 to be linked to the denial of his Article 8 rights, it was not necessary to independently consider this claim.

Article 41

The Court awarded the applicant €12,000 in respect of non-pecuniary damage, and €9,268.60 for costs and expenses.

The EU-US Privacy Shield, providing a transfer mechanism for personal data from EU Member States to the US, was held to be invalid as it was insufficient to ensure adequate protections for personal data. Standard contractual clauses remained a valid transfer mechanism in principle, but data controllers must undertake additional work to ensure that the third country has equivalent data protections.

JUDGMENT OF THE COURT (GRAND CHAMBER) IN THE CASE OF

DATA PROTECTION COMMISSIONER v. FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

(Case No. C-311/18)
16 July 2020

1. Principal facts

This case was a preliminary reference emanating from the High Court (Ireland) on the EU adequacy decision in respect of transfers of personal data to the US (the "EU-US Privacy Shield")[275] and EU standard contractual clauses for the transfer of personal data to third countries.

The General Data Protection Regulation ("GDPR") restricts transfers of personal data out of the EU but provides for a number of data transfer mechanisms that data controllers can rely on to validly transfer personal data from a Member State to third countries (as did the Data Protection Directive (Directive 95/46/EC) before it). The GDPR permits transfers that are covered by a decision by the European Commission that the third country provides an adequate level of protection for personal data (an "adequacy decision"). In the absence of an adequacy decision, the most common alternative is the use of standard contractual clauses ("SCCs") approved by the European Commission.

Maximillian Schrems, an Austrian national, had been using the Facebook social media platform since 2008. In 2013, Schrems filed a complaint to the Irish Data Commissioner (the "Commissioner") requesting that Facebook Ireland be prohibited from transferring his personal data to the United States, on the grounds that the European Commission's adequacy decision in relation to US entities signed up to the 'Safe Harbor' framework was invalid as law and practice in force in the US did not ensure adequate protection of personal data, in particular

[275] Pursuant to Commission Implementing Decision (EU) 2016/1250.

against state surveillance activities.

In a judgment of 6 October 2015 in *Schrems I* (Case No. C-362/14), Safe Harbor was declared invalid. On referral of the case back to the referring court, the High Court (Ireland) referred the decision back to the Commissioner. In the course of the Commissioner's investigations, it transpired that a large part of the personal data had been transferred to the US under standard contractual clauses in the annex to Decision 2010/87/EU, as amended by Commission Implementing Decision (EU) 2016/2297 (the "SCC Decision") rather than in reliance on the Safe Harbor, and the Commissioner invited Schrems to reformulate his complaint.

Having done so, the validity of the SCC Decision was brought into question, and a further preliminary reference was made by the High Court (Ireland).

The case turned on the validity of the SCC Decision and the adequacy decision in relation to the EU-US Privacy Shield (a successor framework to Safe Harbor) given the basic principle that data transferred to a third country must be afforded adequate protections compared to those guaranteed within the EU by the GDPR.

2. Questions posed by the national court

The High Court (Ireland) first asked whether EU law applies to a transfer of personal data by a private company from a Member State to a third country pursuant to the SCC Decision, where that personal data may be further processed for the purposes of national security and law enforcement in the third country, notwithstanding Article 4(2) of the TEU and Article 3(2) of the Data Protection Directive.

Secondly, the national court asked what level of protection was required by Articles 46(1) and 46(2)(c) of the GDPR in respect of a transfer of personal data to a third country on the basis of SCCs.

Thirdly, the national court asked whether Articles 58(2)(f) and (j) of the GDPR means that a competent supervisory authority is required to suspend or prohibit the transfer of personal data to a third country pursuant to SCCs if, in the view of the supervisory authority, those clauses are not or cannot be complied with in the third country and the protection of data transferred (as required by the GDPR and the Charter of Fundamental Rights of the European Union ("CFR")) cannot be ensured; and whether the exercise of such powers is limited to exceptional cases.

Finally, the national court asked whether the SCC Decision was valid, in light of Articles 7, 8 and 47 of the CFR; and (although the reference was made prior to its adoption), in essence, whether the EU-US Privacy Shield ensured an adequate level of protection.

3. Decision of the CJEU

In response to claims that the preliminary reference was inadmissible due to the repeal of the Data Protection Directive and its replacement by the GDPR, the CJEU held that the Data Protection Directive was in force when the preliminary reference was made, and that the GDPR in essence reproduces various relevant articles of the Data Protection Directive. The CJEU reached its judgment on the basis of the GDPR rather than its predecessor directive because the Irish Data Commissioner had not reached a final decision on the *Schrems* complaint (which related to future processing) when the GDPR entered into force.

With regard to the first question, the CJEU ruled that, notwithstanding limitations on the scope of the GDPR in relation to national security and defence, the GDPR does apply to the transfer of personal data by a private company in a Member State to a private company in a third country, irrespective of whether, at the time of transfer or later, the data is liable to be processed by the authorities of the third country for the purposes of public security, defence or state security. Processing by a third party for such purposes could not fall outside the scope of the GDPR because, amongst other reasons, the European Commission is expressly required to have regard to a third country's laws "*including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation*" when assessing the adequacy of that third country's protections (Article 45(2)(a) GDPR).

With regard to the second question, the CJEU ruled that appropriate safeguards, enforceable rights and effective legal remedies required by Articles 46(1) and 46(2)(c) GDPR must ensure that data subjects whose personal data is transferred to a third country under SCCs are afforded a level of protection "essentially equivalent" to those guaranteed under the GDPR read in light of the CFR. In assessing equivalence, both the contractual clauses agreed between the data controller/processor and the third country recipient, and the legal system of the third country (including the non-exhaustive factors set out in Article 45(2) GDPR), must be taken into account.

With regard to the third question, in the absence of a valid adequacy decision from the European Commission, a Member State's supervisory authority is required to suspend or prohibit a transfer of data to a third country under the European Commission's SCCs if, in the view of the supervisory authority and in light of the circumstances of the transfer, the SCCs are not or cannot be complied with in the third country and the requisite level of protection cannot be ensured. The supervisory authorities of Member States are responsible for monitoring compliance with the GDPR and ensuring its enforcement. Even where there is an adequacy decision, a competent national supervisory authority must be able to independently assess whether the transfer of the relevant data complies with the GDPR and, where relevant, bring an action before national courts or make a reference for a preliminary ruling by the CJEU as to the validity of the adequacy decision. Where there is an *adequacy decision*, however, a national supervisory authority is not empowered to suspend or prohibit transfers on the ground that it considers, contrary to a European Commission decision, that adequate levels of protection are not ensured unless and until the CJEU declares the adequacy decision invalid.

While the SCC Decision was ruled to remain valid, the EU-US Privacy Shield was ruled to be invalid. The grounds on which the adequacy of the EU-US Privacy Shield's protections were called into question centred on US surveillance programmes PRISM and UPSTREAM, requiring various US public authorities to be provided bulk access to certain personal data of non-US citizens located outside the US. The data processed was found to be beyond what is considered strictly necessary for EU law purposes. In particular, it was noted that non-US citizens were not afforded the same actionable judicial review rights as US citizens against US authorities relating to their personal data. An ombudsperson mechanism had been introduced to the EU-US Privacy Shield, but the CJEU found that this was inadequate to remedy the deficiencies found in the judicial protection of data subjects whose personal data is transferred to the US as the ombudsperson had no powers to adopt a decision that would bind the US intelligence services. This absence of judicial protection meant that the EU-US Privacy Shield did not ensure "essential equivalence" to the protections afforded under the GDPR, and the EU-US Privacy Shield was therefore incompatible with the GDPR and invalid.

As the SCCs are only binding on a controller/processor in the EU and the third country recipient of data transfers (as parties to the contract), and not to the authorities in the relevant third country, the CJEU held that there are circumstances in which SCCs may be insufficient to ensure the adequate protection of data;

for example, where the laws of the third country enable public authorities to disproportionately interfere with the rights of data subjects. It was noted that the SCC data transfer mechanism differed from the adequacy decision mechanism by not involving an examination of the legislation of the third country, and that it was the responsibility of controllers/processors established in the EU to determine on a case-by-case basis whether additional safeguards were required to supplement those provided by the SCCs in order to ensure a level of protection essentially equivalent to that in the EU. Under the SCCs, a data importer in a third country was obliged to notify the EU controller of any inability to comply with the SCCs.

Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the CFR. Hence, Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary. Directive 2006/24 was therefore held to be invalid.

JUDGMENT OF THE COURT (GRAND CHAMBER) IN THE CASE OF

DIGITAL RIGHTS IRELAND LTD v. MINISTER FOR COMMUNICATIONS, MARINE AND NATURAL RESOURCES AND OTHERS AND KÄRNTNER LANDESREGIERUNG AND OTHERS

(Case Nos C-293/12 and C-594/12)
8 April 2014

1. Principal facts

These cases were preliminary references emanating from the High Court (Ireland) and the Verfassungsgerichtshof (Austria) concerning obligations placed on providers of publicly available electronic communications services or of public communications networks to retain traffic and location data which are generated or processed by them and the validity of Directive 2006/24/EC of 15 March 2006 (the "Data Retention Directive").

The main aim of the Data Retention Directive was to harmonise the domestic legislation of Member States relating to the obligations imposed on providers of publicly available electronic communications services or of public communications networks concerning the retention of certain data. This was to ensure that data was available for the prevention, investigation, detection and prosecution of serious crimes. Hence, pursuant to the Data Retention Directive, providers were obliged to retain data for the period of between six months and two years from the date of the communication. In addition, the Data Retention Directive required the retention of metadata (also known as traffic data), but it did not require the retention of the content of the communication between subscribers or users.

2. Questions posed by the national court

In case C-293/12, Digital Rights Ireland Ltd, an Irish digital rights organisation, challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications. The organisation requested the Irish High Court to declare the Data Retention Directive and Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 invalid. Given the Irish High Court was unable to address the questions relating to national law without the validity of the Data Retention Directive being examined, it chose to stay proceedings and to refer various questions to the CJEU for further consideration.

In terms of the request for a preliminary ruling made by the Verfassungsgerichtshof (Austrian Constitutional Court) in Case C-594/12, the Kärntner Landesregierung (Government of the Province of Carinthia), Mr Seitlinger, Mr Tschohl and 11,128 other applicants challenged the compatibility with the Federal Constitutional Law (*Bundes-Verfassungsgesetz*) of the law transposing the Data Retention Directive into Austrian national law. They argued that their fundamental rights were infringed. The referring court expressed uncertainties about whether the Data Retention Directive could achieve its objectives and questioned the proportionality of its interference with the fundamental rights concerned.

3. Decision of the CJEU

The CJEU found it necessary to address the question of the validity of the Data Retention Directive in light of the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("CFR").

The CJEU had no difficulty finding that the Data Retention Directive interfered with the protection of those two rights, noting that "*the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*". Its analysis therefore concentrated on whether such an interference could be justified.

The rules on justifying interferences with CFR rights are set out in Article 52(1) of the CFR. Any limitation upon CFR rights and freedoms must be provided

for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

The CJEU referred to the public interest justification, namely public safety, for the restriction of the CFR rights at issue. It also noted that the essence of the rights was not affected because, with regard to the right to privacy, the content of communications was not recorded and, with regard to the right to data protection, certain data processing and data security rules had to be respected.

As a consequence, the key issue in the CJEU's ruling was the proportionality of the interference with CFR rights. The CJEU indicated that judicial review of the EU legislature's discretion should be strict in this case, applying factors such as the area of law concerned, the nature of the right, the nature and seriousness of the infringement, and the objective pursued.

The first aspect of proportionality, namely the appropriateness of the interference with the right for obtaining the objective, was fulfilled as the data concerned might be useful to investigations. However, the CJEU found that the Data Retention Directive was problematic when it comes to the second facet of proportionality, i.e., the necessity of the measure in question. The CJEU ruled that the important objective of investigating serious crime and terrorism did not justify data retention.

The CJEU's analysis subsequently proceeded by setting out the general importance of safeguards as regards the protection of privacy and data protection rights building upon the case law of the European Court of Human Rights. These safeguards are even more necessary when data is processed automatically with a risk of unlawful access.

Applying this test, the CJEU gave three reasons why the rules in the Data Retention Directive were not strictly necessary. Firstly, the Data Retention Directive had an extremely broad scope, given that it applied to all means of electronic communication, which have widespread and growing importance in everyday life, without being sufficiently targeted. What is more, the CJEU said that it entails an interference with the fundamental rights of practically the entire European population.

Secondly, besides the general absence of limits in the Data Retention Directive, it failed to limit access to the data concerned by law enforcement authorities and the subsequent use of that data. In particular, the Data Retention Directive did not restrict the purpose of subsequent access to that data, it did not limit the number of persons who could access the data, and it did not control access to the data by means of a court or other independent administrative authority.

Lastly, the Data Retention Directive did not set out sufficient safeguards in respect of the data retention period, the protection of the data from unlawful access and use, the absence of an obligation to destroy the data, as well as the omission of a requirement to retain the data within the EU only.

The rule prohibiting general and indiscriminate metadata retention remains, but legislative measures enabling the collection of data where there is a serious threat to national security can be permitted where limited in time to what is strictly necessary and compatible with fundamental freedoms and other general principles of EU law.

JUDGMENT OF THE COURT (GRAND CHAMBER) IN THE JOINED CASES OF

LA QUADRATURE DU NET AND OTHERS V PREMIER MINISTRE AND OTHERS, FRENCH DATA NETWORK AND OTHERS v. PREMIER MINISTRE AND OTHERS, AS WELL AS ORDRE DES BARREAUX FRANCOPHONES ET GERMANOPHONE AND OTHERS V CONSEIL DES MINISTRES

(Case Nos C-511/18, C-512/18 and C-520/18)
6 October 2020

1. Principal facts

These three cases were preliminary references emanating, respectively, from the Conseil d'État (Council of State, France) and the Cour Constitutionelle (Constitutional Court, Belgium) on the interpretation of Article 15(1) of Directive 2002/58/EC of 12 July 2002 (the "e-Privacy Directive"). Article 15(1) of the e-Privacy Directive provides that Member States may legislate to restrict the rights and obligations set out in certain other articles of the Directive, including the limited retention of data, where necessary, appropriate and proportionate to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of electronic communication systems.

The first case concerned a number of advocacy groups and non-profit organisations in France bringing applications before the Conseil d'État for the annulment of several French decrees that they claimed infringed the French Constitution and European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") as well as the e-Privacy Directive and Directive 2000/31/EC of 8 June 2000 (the "Electronic Commerce Directive"), read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights ("CFR")..

The second case, brought largely by the same group of applicants as above, concerned an application to annul legislative texts allegedly infringing Article 15(1) of the e-Privacy Directive (read in light of Articles 7, 8 and 11 of the CFR) by imposing an obligation of general indiscriminate retention of communications data for judicial purposes relating to criminal offences.

The third case concerned a number of organisations bringing various actions before the Constitutional Court in Belgium for the annulment of Belgian law requiring the retention of data. The applicants claimed that the law failed to provide adequate guarantees for the protection of retained data, infringing the Belgian Constitution, various provisions of the ECHR, International Covenant on Civil and Political Rights, and the Article 4(2) Treaty of the European Union ("TEU").

2. Questions posed by the national courts

The referring national Courts in each of the three cases asked, in essence, whether Article 15(1) of the e-Privacy Directive precludes national legislation imposing an obligation on providers of electronic communications services to require the general and indiscriminate retention of traffic and location data.

The Conseil d'État in Case No. C-511/18 further asked whether Article 15(1) of the e-Privacy Directive precludes national legislation which requires providers of electronic communications services to implement on their networks measures allowing (i) automatic analysis and real-time collection of traffic and location data; and (ii) real-time collection of technical data concerning the location of the terminal equipment used (and not providing for persons concerned by that processing and collection to be notified of it).

In Case No. C-512/18, the Conseil d'État also asked whether the provisions of the Electronic Commerce Directive, read in light of Articles 6, 7, 8, 11 and 52(1) of the CFR, preclude national legislation which requires online communication services providers and hosting service providers to retain, generally and indiscriminately, personal data relating to those services.

In Case No. C-520/18, the Cour Constitutionelle asked, in essence, whether a national court may apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make in respect of national legislation imposing on electronic communications services providers

(with a view to pursuing national security safeguarding and crime combatting objectives) an obligation requiring the general and indiscriminate retention of traffic and location data, on account of the fact that the legislation is incompatible with Article 15(1) of the e-Privacy Directive, read in light of Articles 7, 8, 11 and 52(1) of the CFR.

3. Decision of the CJEU

The CJEU held that national legislation requiring providers of electronic communications services to retain traffic and location data for the purposes of protecting against serious threats to national security and combatting crime are within scope of the e-Privacy Directive. The Court stated that the purpose of the directive is to protect users from personal data and privacy risks, including prohibitions on storing personal data without users' consent, and that derogation from the relevant provisions necessarily raises issues of compatibility with the Articles of the CFR relating to privacy, the protection of personal data and freedom of expression.

In relation to the first and third questions, the Court concluded that in exercising powers pursuant to either Article 15(1) of the e-Privacy Directive or Article 23 of the Electronic Commerce Directive, Member States are precluded from introducing legislative measures which provide for general and indiscriminate retention of traffic and location data as a preventative measure or which require online communication services and hosting service providers to retain, generally and indiscriminately, personal data relating to those services. To do so, given the risk of profiling, would undermine respect for private life, amongst other CFR rights, and derogation would only be permissible subject to the requirement of proportionality and where strictly necessary. It was not necessary for the data to be used; its mere retention (considering the quantities of data concerned in the context of electronic communications services) risked abuse and unlawful access.

However, Member States may legislate for the retention of traffic and location data in certain circumstances in connection with national security, combatting serious crime and/or preventing serious threats to public security, using clear and precise rules in compliance with the CFR and with effective safeguards against the risks of abuse. For example, mechanisms to enable state authorities to instruct electronic communications services to retain data in response to a genuine or foreseeable national security threat are permissible, as is the targeted retention of traffic and location data which is limited in scope and time based on objective and

non-discriminatory criteria and to what is strictly necessary. Data from which it is not possible to profile private lives is also permitted to be retained.

With regard to automated analysis and real-time collection without notification, the Court held that Article 15(1) of the e-Privacy Directive read in conjunction with Articles 7, 8, 11 and 52(1) of the CFR does not preclude national legislation requiring electronic communications services to automatically analyse or collect in real time traffic and location data or technical data concerning the location of terminal equipment used. However, automated analysis should be limited to situations in which a Member State faces a serious threat to national security that is genuine, present or foreseeable, and there must be a means of effective review by a court or other administrative body whose decision is binding in order to verify the justification of that measure and the observation of the conditions and safeguards that are put in place. Likewise, real-time collection should be limited to persons in respect of whom there is a valid reason to suspect that they are involved in terrorist activities, subject to prior review by a court or other administrative body whose decision is binding in order to ensure that real-time collection is authorised only within the limits of what is strictly necessary.

Finally, with regard to maintaining temporal limitations on the effect of a declaration of illegality in relation to national legislation found to be incompatible with EU law, the CJEU held that national courts may not apply such provisions. EU law has primacy over the law of Member States, and unlike a breach of procedural obligations, a failure to comply with Article 15(1) of the e-Privacy Directive involves imposing on electronic communications services providers obligations which seriously interfere with fundamental rights of persons whose data is retained.

National criminal courts are required to disregard information and evidence obtained by means of general and indiscriminate retention of traffic and location data in breach of EU law in criminal proceedings against persons who are not in a position to comment effectively on the information and/or evidence, and the information/evidence pertains to a field of which the judges have no knowledge and where it is likely to have a preponderant influence on findings of fact. However, the CJEU found that, save where the above applies, it is (in principle) for national law alone to determine rules regarding the admissibility and assessment of information obtained in criminal proceedings by such retention of data in breach of EU law.

EU law precludes national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union, departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. The application of the system established by Directive 2016/681 must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application.

JUDGMENT OF THE COURT (GRAND CHAMBER) IN THE CASE OF

LIGUE DES DROITS HUMAINS ASBL v. CONSEIL DES MINISTRES

(Case No. C-817/19)
21 June 2022

1. Principal facts

This case was a preliminary reference emanating from the Cour constitutionnelle (Constitutional Court, Belgium) on the interpretation of Directive (EU) 2016/681 of 27 April 2016 (the "PNR Directive"), which concerns the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

The PNR Directive was adopted as a consequence of terrorist attacks in Paris in 2015 and Brussels in 2016. It creates an EU legal framework for the collection and use of passengers' personal data on flights to or from third countries. Member States have the power to apply the PNR Directive to flights within the EU. Under the PNR Directive, Member States designate a competent authority to act as its Passenger Information Unit (PIU).

Furthermore, Member States must impose a legal obligation on air carriers to transfer the PNR data listed in Annex I of the PNR Directive by electronic means to the database of the PIU. PNR data may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious

crime. PNR data must be de-personalised six months after receipt and deleted after the period of five years.

However, civil liberties organisations argued that data retention under the PNR Directive by law enforcement and other authorities is an invasive and unjustified encroachment on the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights ("CFR"). In 2017, Belgium-based *Ligue des droits humains* (LDH) and other rights groups challenged the PNR Directive at a Belgian court. They contended that the PNR Directive allows the collection of too much data which could result in mass surveillance, discrimination and profiling.

2. Questions posed by the national court

The request for a preliminary ruling made in the proceedings between the LDH and the *Conseil des ministres* (Council of Ministers, Belgium) related to the legality of the *loi du 25 décembre 2016, relative au traitement des données des passagers* (Law of 25 December 2016 on the processing of passenger data).

In its request the Belgian Constitutional Court raised several fundamental questions about the compatibility of the PNR Directive with Articles 7, 8 and 52(1) of the CFR.

Article 52(1) of the CFR deals with the rules on justifying interferences with CFR rights and freedoms. Any limitation upon CFR rights and freedoms must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

Further, the referring court asked specific questions about the Belgian legislation which transposes the PNR Directive. The Belgian legislation includes activities of intelligence and security services within the remit of the purposes for which PNR data is processed and grants power to the PIU to authorise access to PNR data older than six months.

3. Decision of the CJEU

Considering the validity of the PNR Directive in light of Articles 7, 8 and 52(1) of the CFR, the CJEU reiterated that "*an EU act must be interpreted, as far as*

possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter."

The CJEU found that as the PNR data include information on identified individuals, the various forms of processing to which those data may be subject will affect the right to privacy guaranteed in Article 7 of the CFR. The CJEU also found that the communication of personal data to a third party, such as a public authority, constitutes an interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the CFR, regardless of the subsequent use of the information communicated. It concluded that "*the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services.*"

However, the CJEU said that the PNR Directive's objective to ensure the internal security of the EU and to combat terrorist offences and serious crime constitute objectives of general interest of the EU that are capable of justifying even serious interferences with the rights in question. It also stated that the PNR Directive still respects the essence of the fundamental rights in Articles 7 and 8 of the CFR because the PNR Directive lays down in a precise manner the scope of the limitation on the exercise of the rights in question, the purposes for processing PNR data and detailed rules governing those processing operations.

With regard to the application of the PNR Directive to passengers flying between the EU and third countries, the CJEU held that the PNR Directive does not go beyond what is strictly necessary merely because it imposes on Member States the systematic transfer and advance assessment of the PNR data of all those passengers.

The CJEU also undertook the advance assessment of PNR data by automated processing. It concluded that in order to strengthen the protection of fundamental rights in light of scientific and technological developments, it must be ensured that no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of PNR data. Moreover, the PIU itself may transfer PNR data to those authorities only after individual review by non-automated means. In addition to those verifications which the PIU and the competent authorities are to carry out themselves, the lawfulness of all automated processing must be open

to review by the data protection officer, the national supervisory authority and, in the context of the judicial redress, the national courts.

Subsequently, the CJEU clarified how the advance assessment of PNR data by automated processing must be organised in conformity with the CFR. The only databases against which the PIU may compare PNR data are databases on persons or objects sought or under alert in accordance with the EU, international and national rules applicable to such databases. Such databases must only be used in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

Lastly, the CJEU held that the retention, during the initial period of six months of the PNR data of all air passengers "*without any indication as to their involvement in terrorist offences or serious crime does not appear, as a matter of principle, to go beyond what is strictly necessary, in so far as it allows the necessary searches to be carried out for the purposes of identifying the persons who were not suspected of involvement in terrorist offences or serious crime*."

Conversely, the CJEU held that the five-year period of general retention of PNR data of all air passengers set out in the PNR Directive, without any connection between the PNR data and the objectives of the PNR Directive, "*entails an inherent risk of disproportionate use and abuse*."

Article 15(1) of Directive 2002/58/EC precludes national legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, Article 15(1) of Directive 2002/58/EC, read in light of Articles 7, 8, 11 and 52(1) of the CFR does not preclude certain national legislative measures, provided that those measures ensure by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse

JUDGMENT OF THE COURT (GRAND CHAMBER) IN THE CASE OF

BUNDESREPUBLIK DEUTSCHLAND v. SPACENET AG AND TELEKOM DEUTSCHLAND GMBH

(Case Nos C-793/19 and C-794/19)
20 September 2022

1. Principal facts

This case was a preliminary reference emanating from the Bundesverwaltungsgericht (Federal Administrative Court, Germany) on the general and indiscriminate retention of traffic and location data under Article 15(1) of the e-Privacy Directive.

SpaceNet AG and Telekom Deutschland GmbH operate in the information technology industry in Germany. They offer publicly available broadband network services to individual and commercial customers. Telekom Deutschland also provides telephone services. They issued proceedings in the Verwaltungsgericht Köln (Administrative Court, Cologne, Germany) to challenge the obligation under the Telekommunikationsgesetz (Law on Telecommunications) of 22 June 2004 (the "German Telecommunications Law") to retain, as from 1 July 2017, traffic and location data relating to their customers' telecommunications. On 20 April 2018, the Verwaltungsgericht Köln (Administrative Court, Cologne, Germany) ruled that the data retention obligations were in violation of EU law. Consequently, the Federal Republic to Germany appealed the decisions before the Bundesverwaltungsgericht (Federal Administrative Court, Germany).

Pursuant to the German Telecommunications Law, providers of telecommunications and information technology services are required to retain, on a general and indiscriminate basis most of the traffic and location data of their end users. Location data is to be kept for four weeks, while other data is to be retained for ten weeks. This is for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security.

2. Questions posed by the national court

The CJEU was asked to interpret Article 15(1) of the e-Privacy Directive, read in light of Articles 6 to 8 and 11 and Article 52(1) of the Charter of Fundamental Rights ("CFR") and Article 4(2) Treaty of the European Union ("TEU").

In particular, the German court asked the CJEU whether EU law precludes national legislation requiring internet service providers to retain communications data.

On the basis of previous CJEU cases, the German court queried the legitimacy of the German retention obligation given that it covers less data and a shorter retention period than the national legislation that had already been examined by the CJEU (for instance, in joint cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others*).

The German court argued that those elements of the German Telecommunications Law reduced the risk that the retained data might allow precise conclusions to be drawn in relation to the private life of customers whose data had been retained. Furthermore, the German court was of the opinion that the German Telecommunications Law provides for the protection of retained data against the risks of abuse and unlawful access.

3. Decision of the CJEU

The CJEU ruled that such retention for the purposes of combating serious crime was in contravention of EU law and the CFR as it could enable exact profiling of people's private lives. The ability to draw a profile about a person's life would lead to serious implications irrespective of the retention period or the quantity or nature of the data retained.

However, the CJEU confirmed that EU law does not preclude national legislation which:

- enables providers of telecommunications and information technology services to retain, on a general and indiscriminate basis, traffic and location data for the purposes of safeguarding national security where a Member State is confronted with a serious threat to national security that is genuine and present or foreseeable. Such order must be subject to judicial review, by a court or by an independent administrative body with the power to make binding decisions and which can confirm the existence of such a situation, and ensure that the required conditions and safeguards are met. The instruction can only be given for a limited period of time that is strictly necessary, but may be extended if a threat persists;
- provides for the targeted retention of traffic and location data for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security. Such provision must be limited geographically or to specific categories of people;
- for the purposes of combating serous crime and preventing serious threats to public security, provides for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
- for the purposes of combating serous crime and preventing serious threats to public security, provides for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; or
- for the purposes of combating serious crime and preventing serious threats to public security, provides for recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in the possession of those service providers.

The safeguards provided for by the German Telecommunications Law at issue in the main proceedings are intended to protect the retained data against the risks of abuse and against any unlawful access. However, the CJEU stated that the retention of and access to those data amount to separate interferences with the fundamental rights guaranteed by the CFR. Therefore, the CJEU was of the opinion that a separate justification pursuant to the CFR is required.

Where inaccuracy is claimed in a request for search engine results to be de-referenced, a data subject must prove the manifest inaccuracy of the information it seeks to be de-referenced from a search engine under the right to erasure and a search engine provider is not under an active obligation to investigate. When evaluating a request for thumbnails in search engine image searches to be de-referenced, the thumbnail images should be assessed on the basis of the information directly available from the search engine results, without reference to the context in which the image is displayed on the underlying webpage to which the thumbnail hyperlinks.

JUDGMENT OF THE COURT (GRAND CHAMBER) IN THE CASE OF

GOOGLE (DÉRÉFÉRENCEMENT D'UN CONTENU PRÉTENDUMENT INEXACT)

(Case No. C-460/20)
8 December 2022

1. Principal facts

This case was a preliminary reference emanating from the Bundesgerichtshof (Federal Court of Justice, Germany) on the right to erasure (commonly known as the 'right to be forgotten') and proving inaccuracy when assessing erasure requests.

TU and RE were individuals with interests in various companies. Articles criticising the business model of the companies were published on a website owned by a US company, some of which contained images of TU and RE. The articles and thumbnails of the images were displayed by Google when TU and RE's names, or their company's names, were entered into its search engine. By September 2017 (in respect of the images) and June 2018 (in respect of the articles), the content had ceased to be accessible on the website or on Google's search engine.

The applicants requested Google as data controller of the personal data processed on its search engine to de-reference links to the articles and remove the image thumbnails from its search results, on the grounds that they contained inaccurate claims and defamatory opinions. Google refused, on the basis that the articles and photographs were set in a professional context and stating that it was unaware of the alleged inaccuracy of the information contained in the articles.

In 2015, TU and RE brought an action before the Landgericht Köln (Regional Court, Cologne, Germany) seeking an order for removal of the links and images, which was dismissed in a judgment of 22 November 2017. An appeal to the Oberlandesgericht Köln (Higher Regional Court, Cologne, Germany) was dismissed in November 2018 on the basis that the applicants had not proven that the articles were inaccurate and infringed the law and because Google, being unable to carry out a final assessment, was not required to de-reference them. On further appeal to the Federal Court of Justice, a preliminary reference was submitted on the interpretation of the General Data Protection Regulation ("GDPR").

Data subjects' right to erasure of personal data is subject to exemptions under the GDPR and is therefore not an absolute right. The point in this case was Article 17(3)(a) of the GDPR, where the processing of personal data is necessary for the exercise of the right to freedom of expression and information. In determining whether this exemption applies, a weighing up exercise between the rights in Articles 7 and 8 (respect for private and family life and protection of personal data) and Articles 11 and 16 (freedom of expression and information and freedom to conduct a business) of the Charter of Fundamental Rights of the European Union ("CFR") is required.

2. Questions posed by the national court

The Federal Court of Justice first asked whether, when weighing rights under the CFR for the purpose of examining a de-referencing request made to a search engine operator on the basis of inaccuracy of the linked content, that de-referencing is subject to the condition that the question of the accuracy of the referenced content has been resolved (at least provisionally) by judicial decision.

The national court also asked whether, when images of a data subject are connected to their name on a search engine and displayed as thumbnails (preview images), the original context of the publication of those photographs should be taken into account in conducting the weighing exercise of CFR rights when examining a de-referencing request made to a search engine operator.

3. Decision of the CJEU

The CJEU stated that the accuracy of the referenced content is a relevant factor when assessing the conditions in Article 17(3)(a) of the GDPR and whether the content provider's freedom of expression may override the data subject's

rights to privacy and protection of personal data. It was also noted that factual assertions and value judgements are distinct, as the latter cannot be proven (in accordance with the case law of the European Court of Human Rights). Freedom of expression cannot override the right to privacy where the content at issue is an inaccurate factual statement; where a value judgement is concerned, a more nuanced balancing exercise is required and the scope of the right to erasure is more curtailed.

In respect of the first question relating to proving if information is inaccurate, the CJEU held that there is no condition that the accuracy of the information has been subject to a judicial decision, whether interim or final when an Article 17 GDPR de-referencing request is made to a search engine provider. On the apportionment of responsibility between the data subject and search engine provider in establishing accuracy, the Court held that a search engine operator cannot be required to play an active role in substantiating facts, although they must take into account all the circumstances of the case, and the burden of proof is therefore on the data subject to establish, with "*evidence that, in the light of the circumstances of the particular case, can reasonably be required of him or her to try to find in order to establish*" the "manifest inaccuracy" of the information found in the content (whether a non-minor part or the whole). A search engine provider is obliged to de-reference content where inaccuracy is obvious or there is a judicial decision against the referenced website provider based on a finding of inaccuracy; and a provider is not obliged to de-reference if inaccuracy is not obvious or not subject to such a judicial decision. The Court also stated that it would not be proportionate to de-reference information where only certain information of minor importance in the context of the content as a whole is proven to be inaccurate.

In relation to the first question, the Court also highlighted the importance of data subjects being able to bring the matter before a supervisory or judicial authority where the operator of a search engine does not grant the request for de-referencing, particularly as judicial authorities are best placed to conduct the balancing exercise of rights required. In such circumstances, a search engine provider is obliged to add a warning to the relevant search results, alerting internet users to be existence of the proceedings.

In respect of the second question, relating to thumbnail images, the CJEU held that the informative value of the photographs themselves must be taken into account when balancing freedom of expression with privacy rights (as required

under Article 17(3)(a) of the GDPR). The analysis is not dependent on the context of their publication by the underlying website provider. However, any text element directly accompanying the display of the photographs in the search results should also be considered. The Court noted that the right to privacy is particularly acute in relation to images because a person's image is "*one of the chief attributes of his or her personality*". In addition, an image was stated to be a particularly powerful means of conveying information to internet users, as well as being more open to (mis)interpretation when presented out of context as a thumbnail and therefore to particularly serious interference with the data subject's rights in comparison to text-based information. Account must be taken of the informative value of those photographs regardless of the context of their publication on the internet page from which they are taken, but taking into consideration any text element which directly accompanies the display of those photographs in the search results, and which is capable of casting light on the informative value of those photographs.

Mere infringement of the GDPR does not warrant compensation for non-material damage; damage and causation are required, but there is little clarity on the lower threshold for 'non-material damage'.

JUDGMENT OF THE COURT (THIRD CHAMBER) IN THE CASE OF

UI V ÖSTERREICHISCHE POST (PRÉJUDICE MORAL LIÉ AU TRAITEMENT DE DONNÉES PERSONNELLES)

(Case No. C-300/21)
4 May 2023

1. Principal facts

This case was a preliminary reference emanating from the Oberster Gerichtshof (Supreme Court, Austria) on the interpretation of Article 82(1) of the General Data Protection Regulation ("GDPR") in relation to non-material damage and the compensation of data subjects.

Since 2017, Österreichische Post, the Austrian postal service, had been processing personal data relating to the political beliefs and affinities of Austrian citizens. Österreichische Post used an algorithm to process this data and categorise citizens by actual or likely alignment to specific political parties. The applicant, an Austrian individual, had not consented to such processing and felt great upset, loss of confidence and a feeling of exposure on account of his supposed political opinions being retained by the company.

The applicant brought a data protection claim in the Landesgericht für Zivilrechtssachen Wien (Regional Court for Civil Matters, Vienna, Austria) for injunctive relief against the continued processing of the relevant data and €1,000 compensation for non-material damage under Article 82 GDPR. On 14 July 2020, the injunction was granted but compensation rejected.

On appeal to the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria), the first instance decision was upheld on 9 December 2020. It was noted that under Austrian law, a breach of data protection rules gives rise to a right to compensation only when the damage suffered reaches a given threshold of seriousness. The applicant's negative feelings were of insufficient seriousness to reach this threshold.

The case was appealed to the Oberster Gerichtshof (Austrian Supreme Court), and the appeal was allowed to proceed only in respect of the compensation element (a cross-appeal brought by Österreichische Post on a point of law relating to the injunction granted against it was dismissed by an interim judgment). The Austrian Supreme Court in support of its request for a preliminary ruling from the CJEU considered that the Article 82 GDPR damages provision must be defined in accordance with EU rather than national law (on account of the wording of recital 146), that such damages must be compensatory rather than punitive, and that compensation should be due where there is tangible if minor damage, but not where the damage is completely negligible (as the lower court thought would be the case for "merely unpleasant feelings").

2. Questions posed by the national court

The Austrian Supreme Court first asked whether the award of compensation under Article 82 of the GDPR also requires, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or whether the infringement of provisions of the GDPR in itself sufficient for the award of compensation. In other words, whether mere infringement of the GDPR gives rise to a right to compensation.

Secondly, the national Court asked whether the assessment of the compensation depends on further EU-law requirements in addition to the principles of effectiveness and equivalence.

Finally, the national Court asked whether it is compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence or effect of the infringement of at least some weight that goes beyond the upset caused by that infringement. In other words, whether there is a minimum threshold of damage required for the payment of compensation.

3. Decision of the CJEU

The CJEU stated that Article 82(1) GDPR sets out three conditions for the right to compensation to arise: (i) processing of personal data infringing the provisions of the GDPR; (ii) damage suffered by a data subject; and (iii) a causal link between the unlawful processing and the damage. The terms of Article 82 GDPR are autonomous concepts of EU law and must therefore be interpreted

uniformly by EU Member States, without reference to national law. Comparing the provisions to Articles 77 and 78 (remedies relating to supervisory authorities and infringement) and Articles 83 and 84 (administrative fines and penalties), the Court noted that the use of "damage" wording was indicative of the intended purpose of the provision, being neither punitive nor focused on infringement per se. Mere infringement of the GDPR was therefore held not to be sufficient to confer a right to compensation on the applicant.

Article 82(1) was found to preclude national rules or practices from imposing a threshold of seriousness to the damage required to be suffered by the data subject. The CJEU noted that the concept of damage was to be defined autonomously, was to be broadly interpreted in accordance with recital 146, and that the imposition of a seriousness threshold would risk undermining the coherence of the regulation if the courts of different jurisdictions were permitted to apply different standards for when it would be possible to obtain compensation.

However, it was held that it is for the domestic law of Member States to contain rules for the quantitative assessment of damages in claims for compensation under Article 82, as well as procedural rules for safeguarding the rights of individuals, subject to the overarching principles of equivalence and effectiveness. The Court added that financial compensation must be "full and effective", compensating the damage actually suffered as a result of the infringement in its entirety, without any requirement for punitive damages.

The AIRE Centre

The AIRE Centre is a specialist non-governmental organisation that promotes the implementation of European Law and supports the victims of human rights violations. Its team of international lawyers provides expertise and practical advice on European Union and Council of Europe legal standards and has particular experience in litigation before the European Court of Human Rights in Strasbourg, where it has participated in over 150 cases.

For twenty years now, the AIRE Centre has built an unparalleled reputation in the Western Balkans, operating at all levels of the region's justice systems. It works in close cooperation with ministries of justice, judicial training centres and constitutional and supreme courts to lead, support and assist long term rule of law development and reform projects. The AIRE Centre also cooperates with the NGO sector across the region to help foster legal reform and respect for fundamental rights. The foundation of all its work has always been to ensure that everyone can practically and effectively enjoy their legal rights. In practice this has meant promoting and facilitating the proper implementation of the European Convention on Human Rights, assisting the process of European integration by strengthening the rule of law and ensuring the full recognition of human rights, and encouraging cooperation amongst judges and legal professionals across the region.

Civil Rights Defenders

Civil Rights Defenders is a politically and religiously independent human rights organisation that partners with and supports human rights defenders working in some of the world's most repressive regions. Operating across four continents, the organisation's headquarters is located in Stockholm, with eight regional branch offices worldwide. Through advocacy, litigation, and public campaigns, the organisation defends people's civil and political rights globally, while also acting as Sweden's civil rights watchdog. Civil Rights Defenders was founded as the Swedish Helsinki Committee for Human Rights in 1982.

UK Government

The preparation of this publication has been supported by the UK Government.
Views presented in the publication do not necessarily reflect the official position of the UK Government.