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

19 November 2024

Judicial Seminar 2025

Protecting human rights in a world of Artificial Intelligence, algorithms and big data

Background Document

Contents

Introduction

"*The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard*" (*S. and Marper v. the United Kingdom* [GC], 2008, § 112).

The progress made in technology and science has been unprecedented over the life of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention"). Significant advances in the field of information and digital technologies, and in particular algorithmic and artificial intelligence (AI) systems continue to occur and with increasing frequency. In particular, AI has rapidly evolved from a niche field of computer science to a transformative force which impacts the way we interact with the world and has brought new perspectives to the discussion about the content and application of human rights and freedoms and correlatively about their protection.

The legal landscape surrounding AI is still in its initial stages, both in terms of applicable regulations and case-law. It was only in 2024 that the Council of Europe and the European Union adopted the first legally binding instruments aimed at providing a legal framework for the States to regulate the activities within the lifecycle of AI systems and their impact on human rights. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law is the first-ever international legally binding treaty in this field which requires each Party to ensure that activities within the lifecycle of AI systems are fully consistent with human rights, democracy and the rule of law. The Artificial Intelligence Act, adopted in the same year by the European Union, aims at laying down a uniform legal framework to ensure responsible development and deployment of AI systems, while addressing potential risks to the values protected by the Union, including fundamental rights, democracy and rule of law. Consequently, any analysis of AI and its implications must be approached with an understanding of this evolving legal context and the potential for significant developments in the near future.

Bearing in mind the relevance of the topic and the recent legislative developments, in this year, which marks the 75th anniversary of the ratification of the Convention, the Judicial Seminar aims to discuss some of the most pertinent questions raised by the development and use of AI systems, with a focus on identifying the challenges and opportunities that they represent for the protection of human rights. Within the topic, three sub-themes have been highlighted for discussion during the Seminar: (1) Freedom of expression in the age of Artificial Intelligence, (2) Artificial Intelligence and the right to a fair trial, and (3) Addressing potential discrimination in Artificial Intelligence.

The purpose of this background paper is to highlight the Court's existing case-law pertaining to certain aspects of the three themes selected for discussion during the Seminar, but not in any way to anticipate or prejudge how the Court will decide the individual cases brought before it, potentially raising AI issues.

The background paper begins with an overview of the Council of Europe's standards in the field of AI.

I. Council of Europe/European standards on Artificial Intelligence: setting the scene

A. Council of Europe materials

The Council of Europe has taken a leading role in the reflection and contributed essentially to shaping the legal framework in which the AI systems are meant to operate. The Council of Europe began working on the theme of AI a decade ago and has intensified its efforts in the last years, with several Council of Europe bodies and committees issuing a number of policy documents, recommendations, declarations, guidelines and other legal instruments. A selection of the most recent of those documents has been prepared for the purpose of this background paper (for an overview of the work done so far, or planned, by the intergovernmental committees and other entities of the Council of Europe in the area of AI, see Council of Europe and Artificial Intelligence).

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, September 2024

The Framework Convention on AI was adopted on 17 May 2024 by the Committee of Ministers of the Council of Europe in Strasbourg and opened for signatures on 5 September 2024, on the occasion of the Conference of Ministers of Justice in Vilnius (Lithuania). On that day, ten Parties signed the Framework Convention, including the European Union (on behalf of its twenty-seven member States) and the United States of America. The Framework Convention is the first international legally binding agreement aimed at regulating the entire lifecycle of AI systems and promoting responsible innovation while managing potential risks and ensuring that AI systems are used in ways that are consistent with human rights, democracy, and the rule of law. The Framework Convention on AI is accompanied by the Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law which while not aiming to provide an authoritative interpretation of the text of the Framework Convention, may facilitate the understanding of its provisions. The Framework Convention on AI represents the culmination of the work undertaken by the Council of Europe in the field. In this respect, it is to be noted that in 2019 the Committee of Ministers set up an inter-government Ad Hoc Committee on Artificial Intelligence (CAHAI) and mandated it to examine the feasibility and potential elements of a legal framework for the development, design and application of AI. In its final report delivered in 2021 CAHAI identified possible elements of a legal framework on AI, based on the Council of Europe's standards on human rights, democracy and the rule of law. In 2021 the work of CAHAI was continued by the Committee on Artificial Intelligence (CAI) which was instructed to draft a "Framework Convention on the design, development, use, and decommissioning of artificial intelligence systems based on the Council of Europe standards on human rights, democracy and the rule of law, as well as other relevant international legal standards, and conducive to innovation". In addition, CAI was also tasked to elaborate, by the end of 2024, "a legally non-binding methodology for the Risk and Impact Assessment of AI Systems from the point of view of Human Rights, Democracy and Rule of Law (HUDERIA Methodology)" to support the implementation of the Framework Convention on AI. The purpose of the HUDERIA Methodology is to provide detailed evaluations of the potential and actual impacts that the design, development and application of an AI system could have on human rights and fundamental freedoms, democracy, and the rule of law. HUDERIA Methodology was adopted by the CAI on 28 November 2024.

Application of AI in healthcare and its impact on the 'patient-doctor' relationship, September 2024

This report, issued by the Council of Europe's Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), focuses on selected human rights principles, as referred to in the 'Oviedo Convention', of particular relevance to the relationship, namely patient autonomy, professional standards, self-determination regarding health data, and equitable access to health care.

The report is intended for decision makers, health providers, health professionals and patients (including patient associations), to (i) consider how AI systems are used in healthcare, having regard to their human rights implications; and (ii) develop and strengthen the therapeutic relationship, especially in supporting doctors and, where appropriate, other healthcare professionals in promoting the rights enshrined in the Oviedo Convention. The report addresses AI in healthcare, including applications that are used by health care professionals as well as applications that are used by the patients themselves (apps prescribed by a doctor, but also independently used apps such as symptom checkers or health data trackers).

Guidelines on the responsible implementation of artificial intelligence (AI) systems in journalism, Steering Committee on Media and Information Society (CDMSI), November 2023

These Guidelines are an important contribution to the promotion of a rule of law-based and human rights-compliant public communication sphere. They provide practical guidance to the relevant addressees, in particular news media organisations, but also States, technology providers and digital platforms that disseminate news, detailing how AI systems should be used to support the production of journalism. The Guidelines envisage certain responsibilities for technology providers and platforms, as well as for member States.

Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Gender Equality Commission (GEC) and Steering Committee on Anti-discrimination, Diversity and Inclusion (CDADI), 2023

The study on the impact of AI on equality, gender equality and anti-discrimination investigates the discriminatory risks of algorithmic technologies, the specific legal responses to algorithmic discrimination that can be offered by the Council of Europe, and the potential of these technologies for promoting equality, including gender equality.

Human rights by design - future-proofing human rights protection in the era of AI, Recommendation of the Commissioner for Human Rights, May 2023

This recommendation reviews key challenges faced by member States in protecting and promoting human rights in the use of AI. Member States are encouraged to assess the human rights risks and impacts of AI systems before their use, strengthen transparency guarantees, and ensure independent oversight and access to effective remedies. The recommendation underscores the key role national human rights structures play in ensuring member States safeguard human rights in the design, development, and deployment of AI systems. It also focuses on the need to reinforce supervision and oversight by independent institutions, to promote transparency around AI systems and public awareness about their impact on human rights, and to proactively explore the potential of AI to boost rather than harm human rights protection.

Report on Hate speech and fake news: the impact on the working conditions of local and regional elected representatives, Congress of Local and Regional Authorities, CG(2022)43-11final

This report explores the growing negative phenomenon of the use, on and offline, of hate speech, fake news and intimidations and abuse experienced by local and regional politicians. It delves into how hate speech, fake news and verbal and physical abuse are becoming part of the every-day experiences of local and regional representatives and sets out their implications and effects on their working conditions. The report details how these negative practices are damaging the fabric of local and

regional democracy through the creation of a toxic and intimidating political environment. It suggests measures to be taken at national, regional and local level, to provide protection and support for local and regional representatives confronted with these phenomena.

Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems, Parliamentary Assembly Resolution 2342 (2020)

In this resolution the Parliamentary Assembly of the Council of Europe took note that a large number of applications of AI for use by the police and criminal justice systems had been used, or their introduction was being considered, in Council of Europe member States. The resolution referred in particular to applications allowing for facial recognition, predictive policing, the identification of potential victims of crime, risk assessment in decision making on remand, sentencing and parole, and identification of "cold cases" that could now be solved using modern forensic technology. The Parliamentary Assembly acknowledged that the use of AI systems in policing and criminal justice systems may have significant benefits if they are properly regulated, and urged the member States to base any such future regulations on universally accepted and applicable core ethical principles: (i) transparency, including accessibility and explicability; (ii) justice and fairness, including non-discrimination; (iii) human responsibility for decisions, including liability and the availability of remedies; (iv) safety and security; and (v) privacy and data protection. The Parliamentary Assembly also called upon member States, among other things, to maintain a register of all AI applications in use in the public sector, to conduct initial and periodic, transparent human rights impact assessments of AI applications, establish effective, independent ethical oversight mechanisms for the introduction and operation of AI systems, and ensure judicial review.

Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (CM/Rec(2020)1)

The member States of the Council of Europe must ensure that any design, development and ongoing deployment of algorithmic systems occur in compliance with human rights and fundamental freedoms. When algorithmic systems have the potential to create an adverse human rights impact for an individual, for a particular group or for the population at large, including effects on democratic processes or the rule of law, these impacts engage State obligations and private sector responsibilities with regard to human rights.

The Committee of Ministers recommends the government of member States in particular to: (i) review their legislative frameworks and policies and practices with respect to procurement, design, development and ongoing deployment of algorithmic systems; (ii) ensure through appropriate regulatory and supervisory frameworks related to algorithmic systems, that private sector actors engaged in the design, development and ongoing deployment of such system comply with the applicable laws and fulfil their responsibilities to respect human right; (iii) engage in regular, inclusive and transparent consultation, co-operation and dialogue with all relevant stakeholders; (iv) prioritise the building of expertise in public and private institutions involved in integrating algorithmic systems into multiple aspects of societies with a view to effectively protecting human rights; (v) encourage the implementation of effective and tailored media, information and digital literacy programmes; and (vi) take account of the environmental impact of the development of large-scale digital services.

Guidelines on facial recognition (T-PD(2020)03rev4)

These guidelines, adopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data – Convention 108+ (T-PD), cover uses of facial recognition technologies, including live facial recognition technologies. In accordance with the guidelines, integrating facial recognition technologies into existing surveillance systems poses a

serious risk to the rights to privacy and protection of personal data, as well as to other fundamental rights, since use of these technologies does not always require the awareness or co-operation of the individuals whose biometric data are processed in this way. This is the case, for instance, with the possibility to access digital images of individuals on the internet. In order to prevent such infringements, the guidelines indicate that the parties to Convention 108+ shall ensure that the development and use of facial recognition respect the rights to privacy and personal data protection, thereby strengthening human rights and fundamental freedoms by implementing the principles enshrined in the Convention 108+ in the specific context of facial recognition technologies. The guidelines provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data.

Unboxing AI: 10 steps to protect human rights, Recommendation of the Commissioner for Human Rights, May 2019

This Recommendation on AI and human rights provides practical guidance on the way in which the negative impact of AI systems on human rights can be prevented or mitigated. It is addressed at member States, but the principles concern anyone who significantly influences the development, implementation or effects of an AI system: (i) member States should establish a legal framework that sets out a procedure for public authorities to carry out a human rights impact assessment on AI systems; (ii) State use of AI systems should be governed by open procurement standards, applied in a transparently run process, in which all relevant stakeholders are invited to provide input; (iii) member States should facilitate the effective implementation of human rights standards in the private sector; (iv) the use of an AI system in any decision-making process that has a meaningful impact on a person's human rights needs to be identifiable and transparent; (v) member States should establish a legislative framework for independent and effective oversight over the human rights compliance of the development, deployment and use of AI systems by public authorities and private entities; (vi) discrimination risks must be prevented and mitigated with special attention for groups that have an increased risk of their rights being disproportionately impacted by AI; (vii) the development, training, testing and use of AI system that rely on the processing of personal data must fully secure a person's right to respect for private and family life; (viii) member States should take into account the full spectrum of international human rights standards that may be engaged by the use of AI, in particular regarding freedom of expression, freedom of assembly and association, and the right to work; (ix) member States must establish clear lines of responsibility for human rights violations that may arise at various phases of an AI system lifecycle; and (x) the knowledge and understanding of AI should be promoted in government institutions, independent oversight bodies, national human rights structures, the judiciary and law enforcement, and with the general public.

Guidelines on Artificial Intelligence and Data Protection (T-PD(2019)01)

These Guidelines, adopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, provide a set of baseline measures that governments, AI developers, manufacturers, and service providers should follow to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection: (i) safeguarding the right to the protection of personal data is essential when developing and adopting AI applications that may have consequences on individuals and society; (ii) AI development relying on the processing of personal data should be based on the principles of Convention 108+; (iii) an approached focused on avoiding and mitigating the potential risks of processing personal data is a necessary element of responsible innovation in the field of AI; (iv) a wider view of the possible outcomes of data processing

should be adopted; (v) AI applications must at all times fully respect the rights of data subjects; and (vi) AI applications should allow meaningful control by data subjects over the data processing and related effects on individuals and on society.

European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment (CEPEJ(2018)14)

Adopted in December 2018 by the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, the Charter represents the first European text setting out ethical principles relating to the use of AI in judicial systems. The Charter provides a framework of five principles that can guide public and private stakeholders responsible for the design and deployment of artificial intelligence tools and services that involve the processing of judicial decisions and data: (i) principle of respect for fundamental rights: ensuring that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights; (ii) principle of non-discrimination: preventing the development or intensification of any discrimination between individuals or groups of individuals; (iii) principle of quality and security: using certified sources and intangible data with models elaborated in a multi-disciplinary manner, in a secure technological environment; (iv) principle of transparency, impartiality and fairness: making data processing methods accessible and understandable, authorise external audits; and (v) principle 'under user control': precluding a prescriptive approach and ensuring that users are informed actors and in control of the choices made. CEPEJ is collecting information on AI systems and other key cyberjustice tools applied in the digital transformation of the judiciary (Resource Centre on Cyberjustice and AI - European Commission for the Efficiency of Justice (CEPEJ) (coe.int)).

Guidelines to respect, protect and fulfil the rights of the child in the digital environment (CM/Rec(2018)7)

These Guidelines provide a set of ground rules which can assist states in providing the necessary basis for looking after children's best interests in the world of the digital environment, in particular: (i) review their legislation, policies and practices; (ii) ensure that the recommendation is translated and disseminated as widely as possible among competent authorities and stakeholders; (iii) require business enterprises to meet their responsibility to respect the rights of the child in the digital environment and to take implementing measures, and encourage them to co-operate with relevant State stakeholders, civil society organisations and children; (iv) co-operate with the Council of Europe by creating, implementing and monitoring strategies and programmes that respect, protect and fulfil the rights of the child in the digital environment; and (v) examine the implementation of this recommendation every five years at least. In 2020 Council of Europe released a Handbook for policy makers on the rights of the child in the digital environment aimed to support the implementation of these Guidelines.

2. Other international materials

Artificial Intelligence Act, EU, 2024

The Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828) was formally adopted by the European Council on 21 May 2024 and published in the Official Journal of the European Union on 12 July 2024. The AI Act contains a risk-based classification of AI systems, as follows:

(i) unacceptable risk refers to AI systems which pose a significant threat to safety and fundamental rights (for instance biometric categorisation, social scoring systems, assessing the risk of an individual committing criminal offenses, compiling facial recognition databases, or manipulative AI) and are, for that reason, prohibited; (ii) high risk AI systems are subject to strict regulations; (iii) limited risk AI systems are subject to lighter transparency obligations, such as ensuring that end-users are aware that they are interacting with AI (for instance chatbots or deepfakes); and (iv) minimal risk AI systems, which include the majority of AI applications currently available on the EU single market (for instance AI enabled video games or spam filters) are unregulated.

Recommendation of the Council on Artificial Intelligence, OECD, adopted in 2019 and amended in 2024

The Recommendation aims to foster innovation and trust in AI by promoting the responsible stewardship of trustworthy AI while ensuring respect for human rights and democratic values. It focuses on policy issues that are specific to AI and strives to set a standard that is implementable and flexible enough to stand the test of time in a rapidly evolving field. The Recommendation proposes a common understanding of key terms, such as "AI system", "AI system lifecycle", and "AI actors", for the purposes of the Recommendation. The Recommendation contains the following principles, which are viewed as complementary and considered as a whole: (i) inclusive growth, sustainable development and well-being; (ii) respect for the rule of law, human rights and democratic values, including fairness and privacy; (iii) transparency and explainability; (iv) robustness, security and safety; and (v) accountability. It also contains the following recommendations for national co-operation: (i) investing in AI research and development; (ii) fostering an inclusive AI-enabling ecosystem; (iii) shaping an enabling interoperable governance and policy environment for AI; (iv) building human capacity and preparing for labour market transformation; and (v) international co-operation for trustworthy AI.

Recommendation on the Ethics of Artificial Intelligence, UNESCO, 2021

This Recommendation aims to provide a basis to make AI systems work for the good of humanity, individuals, societies and the environment and ecosystems, and to prevent harm. It also aims at stimulating the peaceful use of AI systems. It devises a set of values and principles that should be respected by all actors in the AI system life cycle and should be promoted through a legislative framework. The values promoted by the recommendation include: (i) respect, protection and promotion of human rights and fundamental freedoms and human dignity; (ii) environment and ecosystem flourishing; (iii) ensuring diversity and inclusiveness; and (iv) living in peaceful, just and interconnected societies. The principles put in place include: (i) proportionality and do no harm; (ii) safety and security; (iii) fairness and non-discrimination; (iv) sustainability; (v) right to privacy and data protection; (vi) human oversight and determination; (vii) transparency and explainability; (viii) responsibility and accountability; (ix) awareness and literacy; and (x) multi-stakeholder and adaptive governance and collaboration.

II. European Court of Human Rights case-law in the age of Artificial Intelligence

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

The Court has not yet had the opportunity to address a significant number of cases concerning the impact of AI on the protection of the rights and freedoms enshrined in the Convention and to test the scope of the complexities and nuances of AI-related issues. However, the established case-law of the Court can offer a basis for considering if and how the principles developed so far might be transferred and applied in the cases raising human rights issues brought about by the use of AI systems.

The case-law presented in this background paper reflects the principles developed by the Court up until this moment and is not meant to anticipate how the Court will deal with future individual cases which may raise issues in the field of AI. The Court will decide those future cases based on their specific factual circumstances, in the light of the relevant domestic legislation and practice of the member State concerned, and within the scope of the relevant European standards that will exist at the time when the case is examined by the Court (*Zavodnik v. Slovenia*, 2015, § 74).

A. Freedom of expression (Article 10 of the Convention)

1. New technologies

Indissociable from democracy, freedom of expression is enshrined in a number of national, European, international, and regional instruments which promote this political system, recognised as the only one capable of guaranteeing the protection of human rights. In its interpretation of Article 10 of the Convention, the Court 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". With the advent of new technologies, the Court acknowledged the important role played by the Internet in enhancing the public's access to news and facilitating the dissemination of information and noted that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression.

In *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, 2009, the applicant company, owner and publisher of *The Times* newspaper, alleged that the rule under United Kingdom law, whereby a new cause of action in libel proceedings accrues each time defamatory material on the Internet is accessed, constituted an unjustifiable and disproportionate restriction on its right to freedom of expression. The applicant newspaper published two articles that were allegedly defamatory of a private individual. Both articles were also uploaded onto *The Times*' website. During the subsequent libel proceedings, the applicant newspaper was required to publish an appropriate notification about the proceedings, to both articles contained in the Internet archive. The Court observed that the maintenance of Internet archives is a critical aspect of the role played by the Internet in enhancing the public's access to news and facilitating the dissemination of information in general. Therefore the Court considered that the Internet archives fall within the ambit of the protection afforded by Article 10 (§ 27). On the merits of the case, the Court found no violation of Article 10, on the grounds that the domestic courts' finding against the applicant had constituted a justified and proportionate restriction on the applicant's right to freedom of expression.

In *Ahmet Yıldırım v. Turkey*, 2012, the applicant owned and ran a website on which he published his academic work and his views on various topics. The website was created using the Google Sites website creation and hosting service. In unrelated criminal proceedings an interim court order was issued ordering the blocking of an offensive website. In the process of implementation of that order,

all access to Google Sites was blocked and the applicant was unable to access his own website. His subsequent attempts to remedy the situation were unsuccessful because of the blocking order issued by the court. In this context, the Court affirmed that the blocking of access to the Internet may be in direct conflict with the actual wording of Article 10 of the Convention, according to which the rights set forth in that Article are secured "regardless of frontiers" (§ 67). With regard to whether the blocking measure was justified, the Court held that such restraints must therefore form part of a legal framework ensuring both tight control over the scope of the ban and effective judicial review to prevent any abuses (§ 64). In the present case, the Court found a violation of Article 10.

In *Delfi AS v. Estonia* [GC], 2015, the applicant company, which runs a news portal run on a commercial basis, complained that it had been held liable by the domestic courts for the offensive comments posted by its readers below one of its online news articles. The applicant company removed the offensive comments about six weeks after their publication. In examining the complaint brought before it under Article 10 of the Convention, the Court, while acknowledging the benefits of the Internet, recognised that these are accompanied by a number of dangers, in that clearly unlawful speech, including defamatory remarks, hate speech and speech inciting violence, can be disseminated as never before, worldwide, in a matter of seconds, and sometimes remain persistently available online (§ 110). The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press (§ 133). The Court applied those principles to the facts of the case and found no violation of Article 10, owing to the fact that the sanction imposed on the applicant, in the concrete circumstances of the case, had been based on relevant and sufficient grounds and had thus not constituted a disproportionate restriction on the applicant's right to freedom of expression (see the section on "Responsible journalism in the online sphere" below).

2. Personal data and facial recognition used for identifying people exercising their freedom of expression

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

The case of *Glukhin v. Russia*, 2023 concerned the use by the police of facial recognition technology to track down a participant in a peaceful protest. The applicant mounted a peaceful solo demonstration without prior notification. The police identified him from the photographs and the video published on social media and subsequently located and arrested him while he was travelling on the underground (§ 86). The Court found that the monitoring of the actions or movements of an individual in a public place using surveillance mechanisms may fall within the scope of Article 8 once any systemic or permanent record of such personal data comes into existence (§ 66). The Court further underlined that personal data revealing political opinions should attract a heightened level of protection (§§ 76 and 86). In the context of implementing facial recognition technology, the Court affirmed that it was essential to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards was all the greater where the use of live facial recognition technology was concerned (§ 82). In the circumstances of the case, the Court found a violation of Article 8.

3. Internet safety and the right to be forgotten

The concept of a "right to be forgotten" has recently emerged in the case-law of the Court and is still under construction. Notwithstanding its novelty, its application in practice has already acquired a number of distinctive features. Generally speaking, the "right to be forgotten" may give rise, in practice, to various measures that can be taken by search engine operators or by news publishers. These 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 *Biancardi v. Italy*, 2021, the Court examined the matter of the de-indexation of sensitive information published on the Internet. The applicant, a former editor-in-chief of an online newspaper, was found liable in civil proceedings for having kept on his newspaper's website an article reporting on a fight in a restaurant, giving details on the related criminal proceedings. The domestic courts noted in particular that the applicant had failed to de-index the tags to the article, meaning that anyone could type into a search engine the name of the restaurant or its owner and have access to sensitive information on the criminal proceedings, despite the owner's request to have the article removed (§§ 67-71). The question of anonymising identities in the on-line article did not arise in this case. The Court noted that not only Internet search engine providers could be obliged to de-index material but also administrators of newspaper or journalistic archives accessible through the Internet, such as the applicant. The Court held that prolonged and easy access to information on the criminal proceedings concerning the restaurant owner (eight months after a formal request to remove it) had breached his right to reputation (§ 70). It thus found that the sanction imposed on the applicant had constituted a justifiable restriction of his freedom of expression and concluded that there was no violation of Article 10.

In *Hurbain v. Belgium* [GC], 2023, a newspaper publisher was ordered by the domestic courts to anonymise, on the grounds of the "right to be forgotten" the electronic online version of an article which had mentioned the full name of a driver responsible for a fatal accident that had taken place many years earlier. The Court engaged with the notion of the "right to be forgotten" and clarified its scope for the purpose of the Convention (§ 187). With the development of technology and communication tools, the Court noted, a growing number of persons sought to protect their interests under what is known as the "right to be forgotten". That was based on the individual's interest in obtaining the erasure or alteration of, or the limitation of access to, past information that affected the way in which he or she was currently perceived. By seeking to have that information disappear, the persons concerned wished 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 (§§ 191-199). The Court thus established that its role was to resolve a conflict between the applicant's rights under Article 10 and the driver's rights under Article 8 of the Convention in the context of an online publication (§ 202). It revisited its existing case-law and adjusted the criteria to be applied for balancing of the respective rights under Article 8 and Article 10 to the issue of continued availability of an electronic archived version of an article disclosing an individual's personal data (§§ 205-11). The Court also reiterated that the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, was certainly higher than that posed by the press, particularly on account of the important role of search engines (§ 236). When applying those criteria to the facts of the case brought before it, the Court found that the national courts had carefully balanced the rights at stake in accordance with the requirements of the Convention and the interference with the applicant's rights guaranteed by Article 10 had been limited to what was strictly necessary and thus, necessary in a democratic society and proportionate. Consequently, it concluded that there had been no violation of Article 10.

4. Responsible journalism in the online sphere

The increased protection afforded to "public watchdogs" and particularly the press under Article 10 is subject to the condition that they comply with the duties and responsibilities connected with the

function of journalist, and the consequent obligation of "responsible journalism". Responsible journalism refers both to the content of the publications and to the journalists' conduct which may not breach the criminal law even with respect to media coverage of matters of serious public concern (*Pentikäinen v. Finland* [GC], 2015, §§ 90-91).

In *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, 2009 (see the section on "New technologies" above), where it was brought to the notice of a newspaper that a libel action had been initiated in respect of that same article published in the written press, the requirement to publish an appropriate qualification to the article contained in the Internet archive was not found to constitute a disproportionate interference with the right to freedom of expression (§ 47). The Court affirmed that 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 was more stringent in the absence of any urgency in publishing the material (§ 45). The Court found no violation of Article 10.

In *Delfi AS v. Estonia* [GC], 2015 (see the section on "New technologies" above), the Court was called upon for the first time to examine a complaint about liability for user-generated comments on an Internet news portal. The Court considered that because of the particular nature of the Internet, the "duties and responsibilities" that were to be conferred on an Internet news portal for the purposes of Article 10 differed to some degree from those of a traditional publisher as regards third-party content (§113). In the present case, the Court considered that there had been no violation of Article 10 of the Convention, finding that the domestic courts' finding of liability against the applicant company had been a justified and proportionate restriction on the portal's freedom of expression, in particular, because: the comments in question had been extreme and had been posted in reaction to an article published by the applicant on its professionally managed news portal run on a commercial basis; the steps taken by the applicant to remove the offensive comments without delay after their publication had been insufficient; and the 320 euro fine had by no means been excessive for the applicant, one of the largest Internet portals in Estonia.

In *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, 2016, a self-regulatory body of Internet content providers and an Internet news portal were held liable for vulgar and offensive online comments posted on their websites following the publication of an opinion criticising the misleading business practices of two real estate websites. The applicants complained about the domestic courts' rulings against them, which had effectively obliged them to moderate the content of comments made by readers on their websites, arguing that that had gone against the essence of free expression on the Internet. The Court reiterated that, although, "because of the particular nature of the Internet, the 'duties and responsibilities' that are to be conferred on an Internet news portal for the purposes of Article 10 may differ to some degree from those of a traditional publisher, as regards third-party content", the fact of providing a forum for the exercise of freedom of expression by enabling the public to impart information and ideas on the Internet had to be assessed in the light of the principles applicable to the press (§§ 61-62). However, the Court considered that the domestic courts, when deciding on the notion of liability in the applicants' case, had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation. Notably, the national authorities had accepted at face value that the impugned comments had been unlawful as being injurious to the reputation of the real estate websites. Consequently, the Court found that there had been a violation of Article 10 of the Convention.

In *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, personal taxation data on 1.2 million individuals were published in a magazine and subsequently disseminated by means of a text messaging service. In the Court's view, the existence of a public interest in providing access to, and allowing the collection of, large amounts of taxation data for journalistic purposes did not necessarily or automatically mean that there was also a public interest in disseminating *en masse* such raw data in unaltered form without any analytical input. A distinction had to be made between the processing of data for journalistic purposes and the dissemination of the raw data to which the

journalists were given privileged access (§ 175). In that context, the fact of prohibiting the mass publication of personal taxation data in a manner incompatible with the national and EU rules on data protection was not, as such, a sanction, despite the fact that, in practice, the limitations imposed on the quantity of the information to be published had potentially rendered some of the applicant companies' business activities less profitable (§ 197).

In *Magyar Jeti Zrt v. Hungary*, 2018, the applicant company was found liable (objective liability) for posting a hyperlink to an interview on YouTube which was later found to contain defamatory content. The applicant company complained that by finding it liable for posting the hyperlink on its website the domestic courts had unduly restricted its rights. The Court underscored in particular the importance of hyperlinking for the smooth operation of the Internet and distinguished the use of hyperlinks as a technique of reporting, from traditional publishing. It reiterated that the very purpose of hyperlinks was, by directing to other pages and web resources, to allow Internet users to navigate to and from material in a network characterised by the availability of an immense amount of information. In the Court's view, hyperlinks contributed to the smooth operation of the Internet by making information accessible through linking it to each other, without, however, exercising any control over the content of the website to which a hyperlink enables access (§§ 73-75). The Court set down elements which need to be considered under Article 10 when looking at whether posting a hyperlink could lead to liability and said that an individual assessment was necessary in each case (§§ 76-77). In the present case, the Court found that the domestic law on objective (strict) liability for disseminating defamatory material had excluded the possibility of any meaningful assessment of the applicant company's right to freedom of expression in a situation where the courts should have had the power to scrutinise the issue carefully. Such objective liability for using a hyperlink could undermine the flow of information on the Internet, dissuading article authors and publishers from using such links if they could not control the information they led to. That could have a chilling effect on freedom of expression on the Internet (§ 83). The Court therefore found that, overall, the applicant company had suffered an undue restriction of its rights and thus concluded that there had been a violation of Article 10.

In *Sanchez v. France* [GC], 2023, which concerned the criminal conviction of a politician for xenophobic remarks posted by third persons on the "wall" of his personal Facebook account during an election campaign, the Court addressed, for the first time, the question of the liability of users of social networks on account of comments by third parties. The Court underlined, in particular, that the applicant's Facebook "wall" was not comparable to a "large professionally managed Internet news portal run on a commercial basis", and rather approached the case in the light of "duties and responsibilities" attributable to politicians when they decided use social networks for political purposes, in particular for an election campaign, by opening fora that were accessible to the public on the Internet in order to receive their reactions and comments (§ 180). In this context, the Court emphasised the fact that an account holder could not claim any right to impunity in his or her use of electronic resources made available on the Internet and that such a person had a duty to act within the confines of conduct that could reasonably be expected of him or her (§ 190). In the latter connection, a degree of notoriety was a relevant factor: a private individual of limited notoriety and representativeness would have fewer duties than a local politician and a candidate standing for election to local office, who in turn would have a lesser burden than a national figure for whom the requirements would necessarily be even heavier, on account of the weight and scope accorded to his or her words and the resources to which he or she would enjoy greater access in order to intervene efficiently on social media platforms (§ 201).

With this in mind, the Court pointed out that the applicant had used his Facebook account in his capacity as a politician and for political purposes, during an election campaign to which the impugned comments were directly related (§ 189). He had furthermore been free to decide whether or not to make access to the "wall" of his Facebook account public. Whilst he could not be reproached for that decision itself, in view of the local and election-related tension at that time, that option had clearly been not without potentially serious consequences, as the applicant must have been aware in the

circumstances (§ 193). Noting that the applicant had not taken timely steps to review the posted comments and delete those that had been clearly unlawful, and that the domestic courts had given reasoned decisions based on the reasonable assessment of the facts (§ 199), the Court concluded that Article 10 had not been violated in that case (§§ 209-10).

5. Data transfers and protection of journalistic sources

Given the vital importance to press freedom of the protection of journalistic sources and of information that could lead to their identification, any interference with the right to protection of such sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake. That finding was also reiterated by the Court with respect to online sources and in the context of bulk interceptions of communications.

In *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, 2011, the applicants (the editorial board and the editor-in-chief of a newspaper) were held jointly liable for an anonymous letter which had been allegedly written by a member of the secret services and which the newspaper had downloaded from a news website and published. The letter contained allegations that senior officials of the Ukrainian security service had engaged in unlawful and corrupt activities and had links to organised crime. The newspaper provided reference to the source of the information and published a comment by the editorial board indicating that the information in the letter might be false and inviting the public to comment. The Court reiterated that, having regard to the role the Internet played in the context of professional media activities and its importance for the exercise of the right to freedom of expression generally, the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions, had seriously hindered the exercise of the vital function of the press as a "public watchdog" (§ 64). Consequently, the Court found a violation of Article 10.

In *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, in the context of bulk interception of communications, intelligence services were allowed to access a large volume of confidential journalistic material inadvertently as a "bycatch" of the bulk operation. The applicants, legal and natural persons, complained about the scope and magnitude of the electronic surveillance programmes operated by the State, of which they considered they had been likely affected. The Court observed that, in the current increasingly digital age, technological capabilities had greatly increased the volume of communications traversing the global Internet and, as a consequence, surveillance which was not targeted directly at individuals had the capacity to have a very wide reach, both within and outside of the territory of the surveilling State. As the examination of a journalist's communications or related communications data by an analyst would be capable of leading to the identification of a source, the Court considered it imperative that domestic law contained robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, even if a journalistic communication or related communications data had not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist, if and when it became apparent that the communication or related communications data contained confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and such examination were "justified by an overriding requirement in the public interest" (§ 450). The Court found a breach of Articles 8 and 10 in respect of the regimes for bulk interception and acquisition of communications data and no breach of both provisions as regards the receipt of intelligence from foreign intelligence services.

6. Free elections (Article 3 of Protocol No. 1 to the Convention)

The Court has emphasised the close relationship between the right to free elections and freedom of expression. Free elections and freedom of expression, and particularly the freedom of political debate,

form the foundation of any democracy. The two rights are inter-related and operate to reinforce each other. It is thus particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely, but free and pluralistic public debate is not limited to the period of elections, it is necessary at all times.

In *Communist Party of Russia and Others v. Russia*, 2012, the Court addressed the question whether the State had a positive obligation under Article 3 of Protocol No. 1 to ensure that coverage by regulated media was objective and compatible with the spirit of "free elections", even in the absence of direct evidence of deliberate manipulation. It found that the existing system of electoral remedies was sufficient to satisfy the State's positive obligation of a procedural nature. As to the substantive aspect of the obligation and the allegation that the State should have ensured neutrality of the audio-visual media, it took the view that certain steps had been taken to guarantee some visibility to opposition parties and candidates on TV and to secure the editorial independence and neutrality of the media. These arrangements had probably not secured *de facto* equality, but it could not be considered established that the State had failed to meet its positive obligations in this area. It thus found no violation of Article 3 of Protocol No. 1.

In the area of political advertisement, in *Animal Defenders International v. the United Kingdom* [GC], 2013, with reference to *Bowman v. the United Kingdom*, §§ 42-43, 1998, the Court reiterated that free and pluralistic public debate was necessary not only during elections but at all times (§§ 106-111). In *Animal Defenders International v. the United Kingdom* [GC], 2013, the applicant, a non-governmental organization, was refused permission to place a television advert, as part of a campaign concerning the treatment of primates, on the grounds that the political nature of the applicant's objectives meant that the broadcasting of the advert fell under the statutory prohibition of political advertising. The Court considered that the reasons adduced by the authorities to justify the prohibition of the applicant's advertisement had been relevant and sufficient and therefore the said prohibition was not found to amount to a disproportionate interference with the applicant's right to freedom of expression. The Court therefore concluded that there had been no violation of Article 10. In *Bowman v. the United Kingdom*, 1998, in which the applicant was criminally prosecuted for expenditure with a view to spreading electoral material in the period immediately preceding elections, the Court found that the total barrier imposed on the applicant's publishing information with a view to influencing the voters had not been necessary in order to achieve the legitimate aim of securing equality between candidates (§ 47). It therefore concluded to that there had been a violation of Article 10.

In *Orlovskaya Iskra v. Russia*, 2017, the applicant organisation was fined for publishing articles in its newspaper qualified as electoral campaign without properly identifying them as such, during the month preceding election day. The Court noted that the impugned publications were related to the applicant's exercise of its freedom to impart information and ideas, and the content of the publications was part of the normal journalistic coverage of a political debate in the print media and consequently found that there was little scope for restrictions (§§ 115-16). The Court considered that the "public watchdog" role of the press was no less pertinent at election time when the press was called to assist the "free expression of the opinion of the people in the choice of the legislature" (§§ 129-31). It thus concluded that there had been a violation of Article 10.

In *Sanchez v. France* [GC], 2023 (see the section on "Responsible journalism in the online sphere" above) a politician was convicted for xenophobic remarks posted by third persons on the "wall" of his personal Facebook account during an election campaign. The Court reiterated that a private individual of limited notoriety and representativeness will have fewer duties than a local politician and a candidate standing for election to local office, who in turn will have a lesser burden than a national figure for whom the requirements will necessarily be even heavier, on account of the weight and scope accorded to his or her words and the resources to which he or she will enjoy greater access in order to intervene efficiently on social media platforms (§ 201). In the circumstances of the case, the Court concluded that Article 10 had not been violated.

In *Glukhin v. Russia*, 2023 (see the section on "Personal data and facial recognition used for identifying people exercising their freedom of expression" above) the applicant was identified by use of facial recognition technology after having participated in a solo protest. In that context, the Court reiterated that personal data revealing political opinions should attract a heightened level of protection (§§ 76 and 86). In the circumstances of the case, the Court found a violation of Article 8.

B. Right to a fair trial (Article 6 of the Convention)

1. Access to court

Referring to the principles of the rule of law and the avoidance of arbitrary power which underlie the Convention, the Court has held that the right of access to a court was an inherent aspect of the safeguards enshrined in Article 6, and was no more absolute in criminal than in civil matters. In several cases the Court examined the impact of new technologies on the individuals' access to court.

In *Farcaş and Others v. Romania* [Committee], 2018 the applicants were creditors of an insolvent company. They complained that they had not been able to keep abreast with the court of proceedings and exercise their procedural rights, owing to the fact that the court documents had been served solely by publication (paper version and electronic §§ 15 and 20) in the Bulletin of Insolvency Proceedings to which they had no access. The Court noted that the cost of the paper-version publication of the Bulletin had been prohibitive for the applicants (§ 36). At the same time, the Court observed that the applicants had not had access to the Internet (§39) and thus had not been able to consult the electronic format of the Bulletin. Consequently, in the absence of alternative means of notification, the Court found that the applicants' right of access to a court had become illusory and concluded to the violation of Article 6.

In *Xavier Lucas v. France*, 2022 the Court found that digital technologies (e-bar/e-justice) could help improve the administration of justice and be harnessed to promote the rights guaranteed by Article 6, thus pursuing a "legitimate aim" (§ 46). The Court also found that the requirement to submit applications electronically/digitally in proceedings involving compulsory representation by counsel was compatible with Article 6 (§ 51). This case concerned a requirement to issue proceedings in the Court of Appeal electronically using the *e-barreau* platform. The Court of Appeal had held that the applicant's paper application to set aside an arbitral award could be entertained on the ground that the online form did not allow users to enter that type of application or the capacity in which the parties were named. However, the Court of Cassation had taken the opposite view, holding that the application should have been filed electronically. The Court considered that a disproportionate burden had been placed on the applicant, upsetting the proper balance between, on the one hand, the legitimate concern of ensuring adherence to the formalities of court proceedings and, on the other, the right of access to a court. Consistent with the applicant's submission that it had been impossible in fact to file the application on the *e-barreau* platform, the Court noted, in particular, that in order to file it electronically on *e-barreau* the applicant's lawyer would have had to fill out the form using inaccurate legal terms. It further observed that the French Government had not shown that specific information about how to lodge such an application had been made available to users. The Court concluded that by giving precedence to the rule that proceedings in the Court of Appeal were to be issued electronically, while disregarding the practical hurdles faced by the applicant in doing so, the Court of Cassation had taken a formalistic approach that was not needed to ensure legal certainty or the proper administration of justice and which therefore had to be regarded as excessive (§ 57). Consequently, the Court held that the applicant's right of access to a court had been breached and found a violation of Article 6.

In *Daugaard Sorensen v. Denmark*, 2024, the applicant reported to the police that she had been raped. The proceedings against the alleged perpetrator were eventually terminated because of errors in the service of decisions by the prosecutor. The decision should have been notified electronically via the

compulsory Digital Post account (*e-Boks*), which would normally succeed instantly, but instead was done via registered post which never reached the alleged perpetrator. The time-limits for the prosecution thus expired (§§ 12-16). The Court found that it had no reason to doubt the efficiency of the system put in place, including the service of notification, but that in the case, because of the procedural errors committed by the Prosecution Service the applicant was not secured an effective prosecution or judicial review in respect of the rape offence that she had reported to the police (§§ 69-70). Consequently, the Court found a violation of the respondent State's positive obligations under Articles 3 and 8 of the Convention.

2. Adversarial hearing (disclosure of evidence) in criminal proceedings

Equality of arms is an inherent feature of a fair trial. It requires that each party be given a reasonable opportunity to present their case under conditions that do not place them at a disadvantage *vis-à-vis* their opponent. This principle requires that a fair balance be struck between the parties, and applies to criminal and civil cases. An issue with regard to access to evidence may arise under the criminal limb of Article 6 insofar as the evidence at issue is relevant for the applicant's case, specifically if it had an important bearing on the charges held against the applicant. In the context of disclosure of evidence, complex issues may arise concerning the disclosure of electronic data, which may constitute a certain mass of information in hands of the prosecution.

In *Sigurður Einarsson and Others v. Iceland*, 2019, the applicants, who had occupied senior positions in a bank that had collapsed in the wake of the 2008 banking crisis in Iceland, were prosecuted for breach of trust or market manipulation and found guilty. They complained that their defence had not been given access to the vast amount of data collected by the prosecution during the investigation phase and, among other things, were unable to have a say in the prosecution's electronic sifting of that data in order to gather relevant information for inclusion in the investigation file. They maintained that no one had reviewed the prosecution's cherry-picking of the documents submitted to the court and that they had been denied access to the full collection of data and the possibility of carrying out a search using the electronic system applied by the prosecutor for searching the electronic data (namely "Clearwell", an e-Discovery system; §§ 16 and 63). The Court accepted that by its nature the "full collection of data" inevitably included a mass of data which was not *prima facie* relevant to the case and that when the prosecution was in possession of a vast volume of unprocessed material it may be legitimate for it to sift the information in order to identify what was likely to be relevant and thus reduce the file to manageable proportions. It considered nevertheless that an important safeguard in the sifting process was to ensure that the defence was provided with an opportunity to be involved in the laying-down of the criteria for determining what might be relevant for disclosure (§ 90). Moreover, as regards identified or tagged data, the Court found that any refusal to allow the defence to have further searches of such data carried out, in principle raised an issue with regard to the provision of adequate facilities for the preparation of the defence (§ 91). On the facts of the case, the Court found that the lack of access to the data in question was not such that the applicants had been denied a fair trial overall and concluded that Article 6 had not been violated on that count.

In *Yüksel Yalçınkaya v. Türkiye* [GC], 2023, the applicant's conviction was based decisively on data concerning his use of an encrypted messaging application, "ByLock", which was analysed by a digital forensic expert (§ 80) but to which the applicant did not have full and timely access (§§ 335-336). The Court acknowledged that electronic evidence had become ubiquitous in criminal trials in view of the increased digitalisation of all aspects of life. It also noted that electronic evidence differed in many respects from traditional forms of evidence, including as regards its nature and the special technologies required for its collection, securing, processing and analysis. Most significantly, the Court noted that electronic evidence raised distinct reliability issues as it was inherently more prone to destruction, damage, alteration or manipulation. The Court also reiterated that the use of untested electronic evidence in criminal proceedings could involve particular difficulties for the judiciary as the nature of the procedure and technology applied to the collection of such evidence was complex and

could therefore diminish the ability of national judges to establish its authenticity, accuracy and integrity. Moreover, the handling of electronic evidence, particularly where it concerned data that were encrypted and/or vast in volume or scope, presented the law enforcement and judicial authorities with serious practical and procedural challenges at both the investigation and trial stages (§ 312). In the circumstances of the case, the Court found a violation of Article 6.

In *A.L. and E.J. v. France* (dec.), 2024, the applicants were prosecuted in the United Kingdom based on their user data from the encrypted telecommunications tool EncroChat that had been remotely retrieved at the French authorities' initiative and shared with the United Kingdom law-enforcement authorities which used them as prosecution evidence in proceedings against the applicants (§§ 100-102). The case, which was brought solely against France, mainly from the perspective of the protection of the applicant's right to respect for their private life, was declared inadmissible by the Court for non-exhaustion of domestic remedies. The Court concluded that there had been a remedy available to the applicants in France by which they might have effectively challenged the data transfer measure, together with the data retrieval measure. The applicants had failed to avail themselves of any remedy in the French courts, however, and had not put forward any particular circumstance that might have exempted them from doing so.

3. The principle of immediacy in criminal proceedings

The Court has held that an important element of fair criminal proceedings is also the possibility of the accused to be confronted with the witness in the presence of the judge who ultimately decides the case. Such a principle of immediacy is an important guarantee in criminal proceedings in which the observations made by the court about the demeanour and credibility of a witness may have important consequences for the accused. Therefore, normally a change in the composition of the trial court after the hearing of an important witness should lead to the rehearing of that witness.

For instance, in *Cutean v. Romania*, 2014, the Court found a violation of Article 6 when none of the judges in the initial panel who had heard the applicant and the witnesses at the first level of jurisdiction had stayed on to continue with the examination of the case. It also noted that the applicant's and the witnesses' statements had constituted relevant evidence for his conviction which had not been directly heard by the judge. In these circumstances, the Court held that the availability of statement transcripts was not able to compensate for the lack of immediacy in the proceedings (§§ 60-73).

In the same vein, in *Cerovšek and Božičnik v. Slovenia*, 2017, the Court found a violation of Article 6 because the reasons for the verdicts against the applicants, that is, their conviction and sentence, had not been given by the judge who had pronounced them but by other judges, who had not participated in the trial (§§ 37-48).

Another example is the case of *Iancu v. Romania*, 2021, in which, although leaving the question of the relevance of the principle of immediacy open, the Court examined under that principle the issue of signing of the judgment by the court's president on behalf of the judge, who had taken part in the examination of the case but then retired before the judgment was delivered (§§ 52-60). The Court found no violation of Article 6 § 1 laying emphasis, in particular, on the following elements: the judgment was adopted by the judicial formation which had examined the case and engaged in direct analysis of the evidence; the judgment was drafted, in accordance with domestic law, by an assistant judge, who had taken part in the hearings and deliberations and who had set out, on behalf of the bench, the grounds for the conviction; the judge who retired had been objectively unable to sign the judgment; the signing of a judgment by all members was not a common standard in all Council of Europe member States; the national legislation limited the admissibility of the signing by the court's president to only those cases where the judge hearing the case was unable to sign the decision; and the president of the court signed the judgment on behalf of the retired judge and not in her (the president's) own name.

An issue related to the principle of immediacy may also arise when the appeal court overturns the decision of a lower court acquitting an applicant of the criminal charges without a fresh examination of the evidence, including the hearing of witnesses or of the applicant himself or herself.

In *Júlíus Þór Sigurþórsson v. Iceland*, 2019, the applicant was charged with criminal price collusion. The main piece of evidence against him was the recording of a telephone conversation, concerning exchanges of information about prices with one of the other accused. The trial court, which took oral statements from the accused, acquitted the applicant. In appeal proceedings before the Supreme Court which had full jurisdiction, the applicant was not heard again. The Supreme Court overturned the acquittal of the applicant and sentenced him to nine months' imprisonment. The Court reiterated that where an appellate court was called upon to examine a case as to the facts and the law and to make a full assessment of the question of the applicant's guilt or innocence, it could not, as a matter of fair trial, properly determine those issues without a direct assessment of the evidence given in person by the accused – who claimed that he had not committed the act alleged to constitute a criminal offence (§ 33). As a rule, the Court stated, when an appellate court overturned an acquittal at first instance, it had to take positive measures to secure the possibility for the accused to be heard; in the alternative, the appellate court had to limit itself to quashing the lower court's acquittal and referring the case back for a retrial (§ 38). The Court concluded to a violation of Article 6 in the circumstances of the case.

4. Bias in the system

In several cases the Court found that the applicants' right of access to a court had been breached because of the domestic courts' bias and prejudice towards the applicants.

For instance, the case of *Moldovan and Others v. Romania (no. 2)*, 2005, was brought by Roma villagers following the killing of fellow Roma and the destruction of their homes. The Court observed that the applicants' ethnicity appeared to have been decisive for the length and the result of the domestic proceedings – including repeated discriminatory remarks made by the authorities and their blank refusal to award non-pecuniary damages (§§ 139-40) and thus found a violation of Article 14 in conjunction with Article 6.

In the same vein, in *Paraskeva Todorova v. Bulgaria*, 2010, the domestic court refused to suspend the prison sentence of an accused woman of Roma ethnic origin, on the ground that she belonged to a minority group for whom a suspended sentence was not a conviction and that such a sentence would not fulfil the function of general and specific prevention (§ 38). The Court found that the applicant had been discriminated against on grounds of her ethnic origin and thus concluded to a violation of Article 14 in conjunction with Article 6.

5. Reasoned decision

According to established case-law reflecting a principle linked to the proper administration of justice, judgments of courts and tribunals should adequately state the reasons on which they are based. Reasoned decisions serve the purpose of demonstrating to the parties that they have been heard, thereby contributing to a more willing acceptance of the decision on their part. In addition, they oblige judges to base their reasoning on objective arguments, and also preserve the rights of the defence.

In *Moreira Ferreira v. Portugal (no. 2)* [GC], 2017, the Supreme Court delivered a judgment dismissing a request for the reopening of a criminal judgment which had been lodged by the applicant following a judgment delivered by the Court finding a violation of Article 6. The Supreme Court held that the Court's judgment was not incompatible with the applicant's conviction and raised no serious doubts about its validity. The applicant contested before the Court the interpretation given by the Supreme Court to that judgment. In that context, the Court reiterated that the extent to which the duty to give reasons applies varied according to the nature of the decision and had to be determined in the light of the circumstances of the case. Without requiring a detailed answer to every argument advanced by

the complainant, that obligation presupposed that parties to judicial proceedings should expect to receive a specific and explicit reply to the arguments which were decisive for the outcome of those proceedings. Moreover, the Court reiterated that in cases relating to interference with rights secured under the Convention, it sought to establish whether the reasons provided for decisions given by the domestic courts had been automatic or stereotypical (§ 84). In applying the principles to the facts of the case, the Court found no violation of Article 6.

In *Yüksel Yalçınkaya v. Türkiye* [GC], 2023 (see the section on "Adversarial hearing" above), where the allegations of the applicant's membership of an armed terrorist organization were decided based decisively on his use of an encrypted messaging application ByLock, the Court considered that the prejudice sustained by the defence on the basis of the foregoing shortcomings had been compounded by the deficiencies in the domestic courts' reasoning *vis-à-vis* the ByLock evidence (§ 337). The Court reiterated that in view of the importance of duly reasoned decisions for the proper administration of justice, the domestic courts' silence on vital matters that went to the heart of the case also raised well-founded concerns on the applicant's part regarding their findings and the conduct of the criminal proceedings "as a matter of form" only (§ 341). The Court found a violation of Article 6.

The importance of reasoned decisions transcends the scope of Article 6 and was reiterated by the Court in respect of other Articles of the Convention. For instance, in *X v. Latvia* [GC], 2013, the Court examined the procedural requirements inherent in Article 8 and found a breach of that provision because of the domestic courts' failure to conduct detailed examination of all relevant points when deciding whether to return a child pursuant to the Hague Convention of 25 October 1980 on the Civil Aspects of International Child Abduction (§§ 119-20). In this respect, the Court reiterated that the domestic courts must make a ruling giving specific reasons in the light of the circumstances of the case. Both a refusal to take account of the parties' arguments and insufficient reasoning in the ruling dismissing such arguments would be contrary to the requirements of Article 8 of the Convention. Due consideration of such allegations, demonstrated by reasoning of the domestic courts that is not automatic and stereotyped, but sufficiently detailed, was necessary. With respect to its own jurisdiction, the Court reiterated that reasoned domestic decisions also enabled it to carry out the European supervision entrusted to it (§ 107). The application of these principles to the circumstances of the case lead to a violation of Article 8.

C. Prohibition of discrimination (Article 14, Article 1of Protocol No. 12 to the Convention)

1. Racial profiling

Discrimination on account of a person's actual or perceived ethnic origin is a form of racial discrimination which, in view of its perilous consequences, requires special vigilance and a vigorous reaction from the authorities. It is for this reason that the authorities must use all available means to combat racism, thereby reinforcing democracy's vision of a society in which diversity is not perceived as a threat but as a source of enrichment. Recently, the Court had the occasion to decide several cases which raised the issue of racial profiling.

In *Basu v. Germany*, 2022, the Court examined the situation of a German national of Indian origin who, together with his daughter, were subjected to an identity check on a train which had just passed the border from the Czech Republic to Germany. The applicant asked the police officers why he was checked, and they said it was a random check. He claimed that the check was prompted by his dark skin colour. In a similar case, *Muhammad v. Spain*, 2022, the applicant and his friend, both Pakistani nationals of the same ethnicity, were requested to identify themselves on a public street allegedly on the sole grounds of their race. In both cases the Court considered that, once there was an arguable claim that an individual may have been targeted by a police identity check on account of racial characteristics and such acts fell into the ambit of Article 8 (right to respect for private and family life), the duty of the authorities to investigate the existence of a possible link between racist attitudes and

a State agent's act was to be considered as implicit in their responsibilities under Article 14 examined in conjunction with Article 8 (*Basu v. Germany*, 2022, § 33 and *Muhammad v. Spain*, 2022, § 68). In the circumstances of the two cases, the Court found a violation of the two provisions combined in *Basu v. Germany*, 2022, but no violation in *Muhammad v. Spain*, 2022.

The case of *Memedova and Others v. North Macedonia*, 2023, concerned ethnic profiling of Roma people by the border guards who refused them the right to leave the country, pursuant to an instruction issued by the Ministry of the Interior to strengthening border controls for organised groups of citizens leaving the country who were potential asylum-seekers. Relying on a number of national and international reports on the matter, the Court concluded that, despite the absence of any discriminatory wording in the internal instructions, the way in which they had been applied in practice by the border officers had resulted in a disproportionate number of Roma being prevented from travelling abroad. The resulting difference in treatment was found to be without any objective and reasonable justification, and thus in breach of Article 14 read in conjunction with Article 2 of Protocol No. 4 to the Convention (freedom of movement).

In *Wa Baile v. Switzerland*, 2024, in which the applicant had been stopped and searched in a railway station allegedly on the sole ground of his dark skin colour, the Court found a violation of the procedural obligations enshrined in Article 14 taken together with Article 8 because of the domestic courts' (criminal and administrative) failure to ascertain whether discriminatory motives had been behind the identity check (§§ 93-103). It further reiterated that the absence of sufficient legal and administrative safeguards ran the risk of discriminatory controls taking place (§ 130) and, in the circumstances of the case, concluded that the Government had not been able to rebut the presumption of discriminatory treatment during the identity check in question (§§ 131-135), thus also finding a violation under the substantive head of Article 14 taken together with Article 8.

2. Bias in the system

The Court has accepted in its case-law that a general policy or measure that has disproportionately prejudicial effects on a particular group may be considered discriminatory notwithstanding that it was not specifically aimed at that group. The Court has also found that discrimination potentially contrary to the Convention may result from a de facto situation.

That was the case in *D.H. and Others v. the Czech Republic* [GC], 2007. The applicants, children of Roma ethnic origin, were placed in special schools for children with mental disability, based on the results of tests applied to all children of school age. Relying on statistical information the applicants claimed that those tests were not adapted to the Roma population in terms of cultural references and mother tongue (§ 27) and for those reasons they resulted in a disproportionate number of Roma children being placed in special schools for children with mental disabilities. The Court took note of the fact that all children had been examined using the same tests which had been conceived for the majority population and had not taken Roma specifics into consideration and found that, at the very least, there was a danger that the tests had been biased and that the results had not been analysed in the light of the particularities and special characteristics of the Roma children who had sat them (§§ 200-201). The Court found a violation of Article 14 taken together with Article 2 of Protocol No. 1 (right to education).

3. Sensitive medical data and access to medical care

The Court reflected in its case-law on the importance, for the protection of a person's right to respect for private life, of the confidentiality of the sensitive medical data. In *I. v. Finland*, 2008, the applicant was an HIV-positive individual whose medical records had allegedly become available to her coworkers. The applicant was a nurse working in a public hospital and received treatment for her infection in the same hospital. She began to suspect that her colleagues were aware of her illness. Because of how the patient register was kept, she was unable to obtain information on who had

accessed her medical file or, for those reasons, compensation for the alleged failure to keep her patient record confidential. The Court found that the confidentiality of health data was crucial not only to protect patients' privacy but also to preserve their confidence in the medical profession and in the health services in general. These considerations were especially valid in the case of HIV infection, given the sensitive issues surrounding the disease (§ 38), and thus found a violation of Article 8. While the case was not examined as one potentially raising an issue of discrimination, it is to be noted that the Court has considered in its case-law that a distinction made on account of an individual's health status, which covers HIV infection, should also be included in the scope of Article 14 and held that people living with HIV were a vulnerable group, due to the prejudice and stigmatisation by the society. Consequently, in such cases the States are afforded only a narrow margin of appreciation in choosing measures that single out groups for differential treatment on the basis of their health (*Kiyutin v. Russia*, 2011, §§ 57 and 64).

In several cases the Court examined allegedly biased approaches in the field of medical care in relation to a personal characteristic of the patient. The cases of *V.C. v. Slovakia*, 2011, and *I.G. and Others v. Slovakia*, 2012, concerned non-consensual sterilisation of Roma women. The Court determined that States had a positive obligation to ensure effective legal safeguards to protect women from non-consensual sterilisation, with a particular emphasis on the protection of reproductive health for women of Roma origin. In this regard, the Court found that Roma women required protection against sterilisation because of a history of non-consensual sterilisation against that vulnerable ethnic minority (*V.C. v. Slovakia*, 2011, §§ 154-155; *I.G. and Others v. Slovakia*, 2012, §§ 143-146). In both cases, the Court found a violation of Article 3 (prohibition of torture) and Article 8 and did not find it necessary to examine separately the applicant's complaint under Article 14.

A similar difference in treatment with respect to medical care may potentially arise because of a person's religious beliefs. While not raising a complaint under Article 14, the case of *Pindo Mulla v. Spain* [GC], 2024 concerned the respect for a patient's indications in terms of medical treatment, when the patient's stance was inspired by her religious beliefs. In that case the applicant, a Jehovah Witness, had registered an advance medical directive recording her express refusal to undergo a blood transfusion of any kind in any healthcare situation, even if her life was in danger, in accordance with her religious beliefs. She also signed an informed consent form refusing a blood transfusion. It was recorded that she would accept any medical treatment that did not involve the use of blood. She was transferred to a different hospital in emergency and eventually received a blood transfusion based on a decision taken by the duty judge. In the application to the duty judge it was indicated that she was a Jehovah's witness, that she had verbally expressed her refusal of all types of treatment and that her condition would be very unstable upon arrival. The Court set out how, in an emergency situation, a patient's autonomy was to be reconciled with their right to life (§§ 138-40, 146-47). The decision to refuse life-saving treatment had to be "clear, specific and unambiguous" and "represent the current position of the patient on the matter" (§ 148). If there were any reasonable grounds to doubt any of these aspects, then there was a duty for health care professionals to make every reasonable effort to determine what the patient would want. If, despite those efforts, the physician – or a national court – was unable to establish that clearly, it was their duty to protect the patient's life by providing essential care (§§ 149-50). The Court underlined that, when a State had decided to put in place a system of advance medical directives that was relied on by patients, it was important that the system functioned effectively (§ 156). Examining the facts of the case brought before it, the Court found a violation of Article 8 read in the light of Article 9 (freedom of thought, conscience and religion).

4. Gender-based cyber-violence

The Court explicitly considered domestic violence to be a form of gender-based violence, which was in turn a form of discrimination against women (*Opuz v. Turkey*, 2009, §§ 184-91 and *Volodina v. Russia*, 2019, § 110). Furthermore, in a series of cases the Court found violations of the applicants' rights in the context of cyber-violence by intimate partners: *Buturugă v. Romania*, 2020 and *Volodina*

v. Russia (no. 2), 2021. While these cases were not decided under Article 14 of the Convention, they were examined in the general context of domestic violence set out in *Opuz v. Turkey*, 2009.

Buturugă v. Romania, 2020, concerned allegations of domestic violence and of violation of the confidentiality of electronic correspondence by the applicant's former husband. The applicant complained of shortcomings in the system for protecting victims of this type of violence and criticised the authorities' refusal to consider her complaint concerning her former husband's breach of the confidentiality of her correspondence. The Court held that the State had failed to fulfil its positive obligations in the field of domestic violence. It found in particular that the national authorities had not addressed the criminal investigation as raising the specific issue of domestic violence, and that they had thereby failed to provide an appropriate response to the seriousness of the facts complained of by the applicant. The investigation into the acts of violence had been defective, and no consideration had been given to the merits of the complaint regarding violation of the confidentiality of correspondence, which was closely linked to the complaint of violence (§§ 75-78). The Court pointed out that cyberbullying was currently recognised as an aspect of violence against women and girls, and that it could take on a variety of forms, including cyber breaches of privacy, intrusion into the victim's computer and the capture, sharing and manipulation of data and images, including private data (§ 74). The Court thus found a violation of Articles 3 and 8.

Volodina v. Russia (no. 2), 2021, concerned allegations of cyberharassment by the applicant's former partner. The applicant alleged that her former partner had used her name, personal details and intimate photographs to create fake social media profiles, had planted a GPS tracker in her handbag, had sent her death threats via social media. The applicant complained that the authorities had failed to protect her and to effectively investigate the allegations made against her former partner. The Court found that the authorities had not complied with their obligations to protect the applicant from severe abuse. Despite having the legal tools available to prosecute the applicant's partner, the authorities had not carried out an effective investigation and had not considered at any point in time what could and should have been done to protect the applicant from recurrent online harassment. The Court thus found a violation of Article 8.

Summary

Bearing in mind the case-law highlighted above and without advancing any considerations on the effects of AI on the future scope and protection of human rights and freedoms, a few general conclusions can be drawn.

Firstly, the intersection of AI and freedom of speech presents a complex and evolving landscape that is reshaping the boundaries of communication in the digital age. The exercise and the protection of freedom of expression have been deeply impacted by the development of digital technologies and, in particular, by the spread of artificial intelligence systems; the dual role of AI as both an enabler and a potential threat to freedom of speech is unquestionable. The necessity to protect both the right to impart and the right to receive information is equally important in the traditional and the digital media (see *Delfi AS v. Estonia* [GC], 2015, in the section on "New technologies" above, and *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, in the section on "Data transfers and protection of journalistic sources" above).

Furthermore, while the potential for the use of AI systems in the judiciary is significant, opinions differ on the extent to which AI can actually be used for judicial work. At the extremes of this discussion are the views which, on one hand, challenge the idea of the necessity of a human court and, on the other, consider that every judicial decision affecting the interests of litigants requires human assessment. Furthermore, there is need to explore how traditional legal skills and knowledge can be used to ensure that AI systems can contribute to improve the efficiency and quality of the judicial process and can serve as productive assistants (or participants) in the judicial process and what is the extent of human intervention needed.

Equally important, in view of the principle that the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective, the right to a fair trial cannot be seen as effective unless the requests and observations of the parties are truly "heard", that is to say, properly examined by the tribunal (*García Ruiz v. Spain* [GC], 1999, § 26). Be that as it may, it is certain that electronic evidence has become ubiquitous in criminal trials in view of the increased digitalisation of all aspects of life (ibid., § 312). In this respect, the European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment and the work of the CEPEJ in mapping the AI systems and other key cyberjustice tools applied in the digital transformation of the judiciary will provide relevant sources of information for the Court (Resource Centre on Cyberjustice and AI – European Commission for the Efficiency of Justice (CEPEJ) (coe.int)).

Lastly, it is recalled that AI systems are not immune to bias and discrimination. These issues can arise from various sources, including biased training data, algorithmic design choices, and the broader societal context in which these systems are deployed. Bearing in mind the scope of the potential application of AI in the day-to-day life, this can have far-reaching consequences for individual rights and can enhance discrepancies and differences constitutive of discrimination. They can exclude certain categories from effective protection or use majority-driven standards oblivious to context sensitivities; a cautionary tale on the dangers of system bias in pre-digital context was told, in this respect, by *D.H. and Others v. the Czech Republic* [GC], 2007 (see the section on "Prohibition of discrimination": "Bias in the system" above). Potential use of AI for cyber-violence between intimate partners is also to be addressed urgently (see *Buturugă v. Romania*, 2020, in the section on "Gender-based cyber-violence" above). In this respect, the work of the Council of Europe Committee of Experts on combating technology-facilitated violence against women and girls (GEC/PC-eVIO) will provide useful input for the work of the Court.

Last but not least, the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, the Explanatory Report to that convention, the HUDERIA Methodology and the future Handbook on Human Rights and artificial intelligence will provide important guidance for assessing the State's obligations in terms of AI and protection of human rights in the coming years.

Annex: List of Cases

Ahmet Yıldırım v. Turkey, no. 3111/10, ECHR 2012
A.L. and E.J. v. France (dec.), nos. 44715/20 and 47930/21, 24 September 2024
Animal Defenders International v. the United Kingdom [GC], no. 48876/08, ECHR 2013 (extracts)

Basu v. Germany, no. 215/19, 18 October 2022
Biancardi v. Italy, no. 77419/16, 25 November 2021
Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, 25 May 2021
Bowman v. the United Kingdom, 19 February 1998, *Reports of Judgments and Decisions* 1998-I
Buturugă v. Romania, no. 56867/15, 11 February 2020

Catt v. the United Kingdom, no. 43514/15, 24 January 2019
Cerovšek and Božičnik v. Slovenia, nos. 68939/12 and 68949/12, 7 March 2017
Communist Party of Russia and Others v. Russia, no. 29400/05, 19 June 2012
Cutean v. Romania, no. 53150/12, 2 December 2014

Daugaard Sorensen v. Denmark, no. 25650/22, 15 October 2024
Delfi AS v. Estonia [GC], no. 64569/09, ECHR 2015
D.H. and Others v. the Czech Republic [GC], no. 57325/00, ECHR 2007-IV

Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, ECHR 2011 (extracts)

Farcaş and Others v. Romania [Committee], no.30502/05, 5 June 2018

García Ruiz v. Spain [GC], no. 30544/96, ECHR 1999-I
Glukhin v. Russia, no. 11519/20, 4 July 2023

Hurbain v. Belgium [GC], no. 57292/16, 4 July 2023

I. v. Finland, no. 20511/03, 17 July 2008
Iancu v. Romania, no. 62915/17, 23 February 2021
I.G. and Others v. Slovakia, no. 15966/04, 13 November 2012

Júlíus Þór Sigurþórsson v. Iceland, no. 38797/17, 16 July 2019

Kiyutin v. Russia, no. 2700/10, ECHR 2011

Magyar Jeti Zrt v. Hungary, no. 11257/16, 4 December 2018
Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, no. 22947/13, 2 February 2016
Memedova and Others v. North Macedonia, nos. 42429/16 and 2 others, 24 October 2023
Moldovan and Others v. Romania (no. 2), nos. 41138/98 and 64320/01, ECHR 2005-VII (extracts)
Moreira Ferreira v. Portugal (no. 2) [GC], no. 19867/12, 11 July 2017
Muhammad v. Spain, no. 34085/17, 18 October 2022

Opuz v. Turkey, no. 33401/02, ECHR 2009
Orlovskaya Iskra v. Russia, no. 42911/08, 21 February 2017

Paraskeva Todorova v. Bulgaria, no. 37193/07, 25 March 2010
Pentikäinen v. Finland [GC], no. 11882/10, ECHR 2015
Pindo Mulla v. Spain [GC], no. 15541/20, 17 September 2024

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008
Sanchez v. France [GC], no. 45581/15, 15 May 2023
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, 27 June 2017
Sigurður Einarsson and Others v. Iceland, no. 39757/15, 4 June 2019

Thlimmenos v. Greece [GC], no. 34369/97, ECHR 2000-IV
Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), nos. 3002/3 and 23676/03, ECHR 2009

V.C. v. Slovakia, no. 18968/07, ECHR 2011 (extracts)
Volodina v. Russia, no. 41261/17, 9 July 2019
Volodina v. Russia (no. 2), no. 40419/19, 14 September 2021

Wa Baile v. Switzerland, nos. 43868/18 and 25883/21, 20 February 2024

X v. Latvia [GC], no. 27853/09, ECHR 2013
Xavier Lucas v. France, no. 15567/20, 9 June 2022

Yüksel Yalçınkaya v. Türkiye [GC], no. 15669/20, 26 September 2023 [GC]

Zavodnik v. Slovenia, no. 53723/13, 21 May 2015