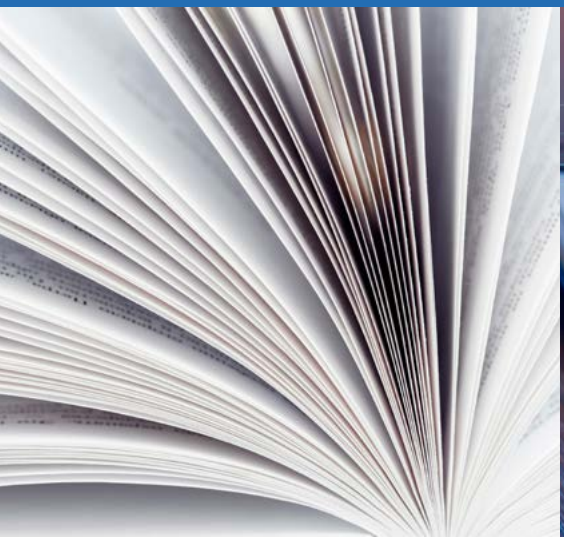
PUBLICATION OF JUDICIAL DECISIONS THE COUNCIL OF EUROPE'S POINTS FOR CONSIDERATION

Fostering transparency of judicial decisions and enhancing the national implementation of the European Convention on Human Rights



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PUBLICATION OF JUDICIAL DECISIONS THE COUNCIL OF EUROPE'S POINTS FOR CONSIDERATION

Fostering transparency of judicial decisions and enhancing the national implementation of the European Convention on Human Rights

Council of Europe

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Photos: Shutterstock

Printed at the Council of Europe

The project Foster Transparency of Judicial Decisions and Enhancing the National Implementation of the European Convention on Human Rights (TJENI) is funded by Iceland, Liechtenstein and Norway through the EEA and Norway Grants Fund for Regional Cooperation.

Iceland Liechtenstein Norway grants
Norway grants

Contents

Introduction

A strong and effective judiciary is one of the foundations of any peaceful, democratic society. Increased consistency, quality and transparency of judicial decisions based on European human rights standards are essential for strengthening human rights and rule of law standards in Council of Europe member states and beyond.

The project Foster Transparency of Judicial Decisions and Enhancing the National Implementation of the European Convention on Human Rights ("TJENI Project") works with the justice systems in the partner states of the project with the aim of strengthening the quality of their judicial decision making through the integration of specialised tools and solutions aimed at improving the consistency, quality and transparency of judicial decisions.

Access to justice is a human right enshrined in Article 6 of the European Convention on Human Rights[1] ("the Convention"). Ensuring online access to judgments increases the transparency of justice systems and public trust in them and contributes to consistency in case law.

The online publication of judicial decisions requires balancing a variety of interests such as the right to personal data protection and the right to publicise judicial decisions to ensure the transparency of the justice system. To balance these interests, in many countries, judicial decisions are anonymised/pseudonymised before their publication, in accordance with legislation and regulations set at national and international levels.

The TJENI Project's objective is to foster transparency of case law and its accessibility to legal professionals and the public and to improve the consistency between national jurisprudence and human rights standards set out in the case law of the European Court of Human Rights ("the Court", "the European Court").

1. The European Convention on Human Rights, available at: www.echr.coe.int/documents/convention_eng.pdf.

This document presents a compilation of existing standards, including those of the Council of Europe, concerning the publication of judicial decisions and related to personal data protection, including those in the case law of the European Court of Human Rights, as well as in recommendations and guidelines adopted by Council of Europe bodies. It synthesises key thematic areas addressed by the TJENI Project:

i. publication of judicial decisions;

ii. personal data protection;

iii. anonymisation and pseudonymisation;

iv. risks related to publication and their mitigation; and

v. information and communication technology (ICT) tools development.

It discusses these thematic areas in the context of the digital era, relating them to the contemporary legal, practical and technological considerations relevant to the publication of judicial decisions today and for future developments. The checklist at the end of the report presents the main issues and questions to be asked deriving from these areas that should be considered by judicial entities in relation to the publication of judicial decisions. This document is a work in progress. It will be updated from time to time as new standards (case law, recommendations, guidelines, etc.) are established.

In Chapter I, the publication of judicial decisions is highlighted as a key element in improving the transparency of the judicial process and the consistency of judicial decisions. In this light, the publication of judicial decisions serves the principle of open justice, which enshrines the need for transparency of judicial processes along with the notion of public oversight and scrutiny of judicial proceedings. In particular, the chapter highlights the interconnections and subsequent interplay between the legal regimes and individual/public interests involved in the publication of judicial decisions; it also considers the various goals and objectives of publication, the methods and entities involved, and the related policies. The chapter reveals the issue of publication as a practical and technical challenge as well as a legal balancing act.

Closely connected to – and deriving from – the publication of judicial decisions, are the concerns and challenges relating to personal data protection. Chapter II explores the relevant international standards and considerations pertinent to the use and protection of personal data in publicly available judicial decisions and explores the distinctions in law and practice between privacy protection and data protection. In doing so, it considers the roles of

judicial entities in the processing and dissemination of protected data, and their related approaches and responsibilities.

Chapter III explores in more detail the techniques of anonymisation and pseudonymisation for the protection of personal data and their application to the publication of judicial decisions. It examines their legal regulation, the specifics of the methodologies and notes their limitations and practical requirements.

This report further delineates the risks related to the publication of judicial decisions and its impact. Chapter IV highlights the technical risks leading to data protection violations and the impact of poor system design on the usefulness of publication. Notably, the increase in the amount of data published in case-law databases requires the introduction of special categorisation tools that allow for the fast thematic search and analysis of data. As will be seen throughout this report, the categorisation of judicial decisions in particular is an important element that can be greatly facilitated by technical solutions, and in turn facilitates a level of automation and control over the administration process that improves efficiency and enables detailed review and data collection.

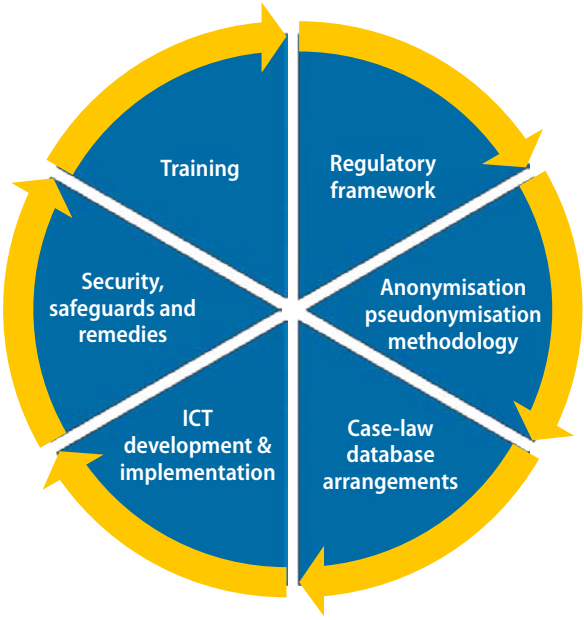
Finally, Chapter V of this report addresses practical aspects that should be considered in the development and integration of technical solutions, including the interoperability of various solutions and systems, and the training of their users.

It is important to note that while specialised digital tools and methodologies can offer increased support in the automatic anonymisation or pseudonymisation of judicial decisions, digital solutions are also playing an increasingly important role in case management systems (CMSs). Notably, automation has long been a standard element of CMSs, which began as a natural replacement for manual approaches to case management. As a result of increasing digital capabilities, CMSs are evolving into more advanced tools that also incorporate functions such as anonymisation/pseudonymisation and categorisation. However, with this evolution, several challenges such as interinstitutional co-ordination and standardisation will have to be addressed. This report highlights the need to ensure a consistent and systematic approach by judicial staff, with corresponding training and implementation.

Each of these above-mentioned thematic areas comprise long-established guidance and factors that need to be implemented for the transparent and efficient administration of justice in line with human rights standards; they remain foundational as new developments in the law, practice and technology arise.

Across these thematic areas, this report will present a compilation of various recommendations, proposed standards and questions that are to be taken into consideration in relation to the provision of public access to judicial decisions. These necessary decisions can be grouped into six main areas, which are the main elements of the publication process:

1. Regulatory framework
2. Anonymisation/pseudonymisation methodology
3. Case-law database arrangements
4. ICT development and implementation
5. Security, safeguards and remedies
6. Training



Chapter 1

Publication of judicial decisions

The publication of judicial decisions is a central element that guarantees the transparency and accountability of the justice system; however, other human rights may be brought into conflict with such publication, notably the rights to privacy and protection of personal data. The publication of judicial decisions is closely linked to the principle of open justice and the concept of open data – where the transparency of the judiciary and judicial process is of key importance. Publication of judicial decisions is a way of satisfying the requirement of Article 6 of the Convention for judgments to be "pronounced publicly" and furthermore reinforces the consistency of case law. At the same time, open data and open justice present unique and evolving challenges to the right to privacy and to data protection rules.

This chapter examines the basis and evolution of the accessibility and publication of judicial decisions, by analysing the jurisprudence of the European Court and the developing standards, and contrasts these with the evolution of the right to privacy and data protection.

Finally, the goals and objectives of publication are considered in light of the need for a clear legal basis guiding such publication. Such a basis is important, as the publication of judicial decisions should never be arbitrary and should be implemented to serve specific purposes including, but not limited to, enhancing transparency, legal certainty, public trust and statistical analysis, as well as improving the quality of decisions and access to legal precedent and relevant case law.

1. Pronouncement and publication of judicial decisions

Open data as a concept is generally understood to mean data in an open format that can be freely used, reused and shared by anyone for any purpose. Open data policies which encourage the wide availability and reuse of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints, and which promote the circulation of information not only for economic operators but primarily for the public, can play an important role in promoting social engagement.[2] The open data movement is radically changing the management, delivery and access to legal and judicial information.

In line with this movement, many countries have introduced tools and platforms for the publication (online and digitally) of jurisprudence with the aim of facilitating and extending access. Even though the open publication of judicial decisions is a movement that started some years ago, Recommendation No. R (95) 11 concerning the selection, processing, presentation and archiving of court decisions in legal information retrieval systems[3] was already adopted in 1995 by the Committee of Ministers of the Council of Europe[4] and addressed to its member states. This recommendation indicates, *inter alia*, that appropriate steps should be taken to ensure that all users have easy access to the relevant legal information retrieval systems that are open to the public. The recommendation establishes that recent judicial decisions should be fed into an automated system regularly and within a reasonable period of time. As far as possible, systems should be updated within a month in the case of supreme court decisions and within three months in the case of decisions by other courts, as from the date of publication of the decision or as from the delivery of the text of the decision to the parties. The updating routines should profit from the most efficient techniques possible, especially reuse of texts already in machine-readable form.

In its Recommendation Rec(2001)3 on the delivery of court and other legal services to the citizen through the use of new technologies,[5] the Committee of Ministers states that it should be as easy as possible to communicate with the courts and other legal organisations (registries, etc.) by means of new technologies. This recommendation envisions, provided that the necessary

2. European Union (2019).
3. Committee of Ministers (1995).
4. The Committee of Ministers is the Council of Europe's statutory decision-making body made up of the ministers for foreign affairs of member states.
5. Committee of Ministers (2001b).

security and privacy requirements are met, the possibility of public access to legal information (for example statute law, case law, regulations), public registers and court proceedings (such as court procedures, rules, case information).

In its 2004 Opinion No. 6 on fair trial with a reasonable time,[6] the Consultative Council of European Judges (CCJE)[7] perceives a need to publish citizens' guides enabling potential litigants to gain a better grasp of the functioning of the judicial institutions, while also informing them of their procedural rights before the courts. It also recommends the general use of computer technology in order to provide members of the public with the same type of information on the functioning of the courts, the means of access to justice, the principal decisions delivered and the statistical results of the courts. In this regard the CCJE considers that the judiciary should make case law, or at least landmark decisions, available on the internet: i. free of charge; ii. in an easily accessible form; and iii. taking account of personal data protection[8].

Publication of judicial decisions is not to be confused with publicity. Publicity of judicial decisions should be understood as meaning their being pronounced or served to the parties, that is, the text of the decision and its legal consequences is provided to persons affected by it. The European Court sets this out as an element of the right to fair trial enshrined in Article 6 of the Convention. Already in 1983, the Court declared in *Pretto and Others v. Italy*[9] that the public character of the proceedings before the judicial bodies referred to in Article 6, paragraph 1, protects litigants against the administration of justice in secret with no public scrutiny. It is also one of the means whereby confidence in the courts, superior and inferior, can be maintained. By rendering the administration of justice visible, publicity contributes to the achievement of the aim of Article 6, paragraph 1, namely a fair trial, the guarantee of which is one of the fundamental principles of any democratic society, within the meaning of the Convention.[10] This principle of the public character of proceedings has been confirmed in the subsequent case law of the European Court.[11]

---

6. CCJE (2004).
7. The CCJE is an advisory body of the Council of Europe on issues relating to the independence, impartiality and competence of judges, composed exclusively of national judges from Council of Europe member states.
8. CCJE (2011), paragraphs 14 and 24.
9. *Pretto and Others v. Italy*, Application No. 7984/77, judgment of 8 December 1983.
10. Ibid., paragraph 21.
11. *Axen v. Germany*, Application No. 8273/78, judgment of 8 December 1983, paragraph 25; *Ryakib Biryukov v. Russia*, Application No. 14810/02, judgment of 17 January 2008, paragraph 30; *Fazliyski v. Bulgaria*, Application No. 40908/05, judgment of 16 April 2013, paragraph 64.

The European Court has recognised that the legislative systems and judicial practice of member states reveal some diversity as to the scope and manner of implementation of both the holding of hearings and the "pronouncement" of judgments.[12] The European Court has pointed out that many state systems have a long-standing tradition of recourse to other means, besides reading out loud, for making public the decisions of all or some of their courts.[13]

Additionally, in light of the requirement of the overall fairness of the process, it cannot be regarded as decisive whether the applicant was able to access the judgments and exercise his rights of appeal. What ultimately matters is whether those judgments are, in some form, made accessible to the public.[14] In the opinion of the Court, the object pursued by Article 6, paragraph 1, could be no less achieved by a deposit in the court registry, making the full text of the judgment available to everyone, than by a reading in open court of a decision.[15]

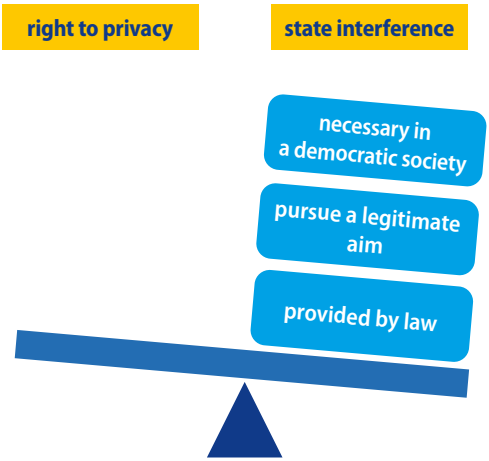
2. Goals and objectives of the publication

Publication of judicial decisions may represent an intrusion into the privacy of the concerned individuals, who could be identified or re-identified in such judicial decisions. Therefore, determining the goals of the publication of judicial decisions is of major importance when the national authorities take decisions about the extent of the publication and the scope of anonymisation/pseudonymisation undertaken to safeguard privacy.

In line with the jurisprudence of the European Court, interference in the rights of individuals by state authorities shall: i. be based on law; ii. pursue a legitimate aim; and iii. be necessary in a democratic society.

The public interest in the publication of judicial decisions (which sometimes has to be balanced against the personal interests of the parties to the proceedings) should be determined through the description of the goals of publication set by the national authorities. In the case of a dispute related to an eventual violation of the right to respect for private and family life (Article 8 of the Convention), the goals of publication should be assessed in light of the particular case and its specific facts.

12. *Pretto and Others v. Italy,* Application No. 7984/77, judgment of 8 December 1983, paragraph 22.
13. Ibid. paragraph 26.
14. *Fazliyski v. Bulgaria*, Application No. 40908/05, judgment of 16 April 2013, paragraph 65.
15. *Pretto and Others v. Italy*, paragraph 27.



The following are possible goals of the publication of judicial decisions.

i. To make the judicial process more transparent and strengthen the rule of law

Wide publication can contribute to greater comprehensibility of case law and transparency of the judicial process. This in turn allows for an increase in the ease of public scrutiny and consequently fosters the rule of law.

ii. To enhance legal certainty

Legal certainty is one of the elements of a fair trial. Timely publication and analysis of court practice and interpretation of legal norms allow access to the positions of the judges on particular legal questions. Awareness of such positions can contribute to the unification of the positions of judges in different regions and enhance uniformity of legal practice and legal certainty. This could contribute to elimination of the problem of inconsistent adjudication in identical situations[16] and secure harmonisation of the relevant case law.[17]

16. *Vinčić and Others v. Serbia*, Application Nos. 44698/06 et al. judgment of 1 December 2009.
17. As a general measure proposed by the national authorities for the execution of the case *Vinčić and Others v. Serbia*, see DH-DD(2017)87.

iii. To strengthen public scrutiny and improve public trust in justice

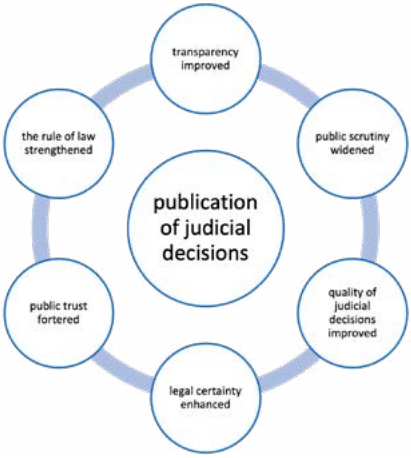
Public interest in the judicial process is indisputable. Also indisputable is the need for public scrutiny of the actions and behaviour of public figures, mainly politicians and representatives of state authorities (public figures inevitably and knowingly lay themselves open to close scrutiny of their every word and deed by both journalists and the public at large).[18] Easy access to the respective judicial decisions on these matters can improve citizens' confidence in governance and the judiciary.

iv. To improve the quality of judicial decisions

A side effect of the publication of judicial decisions is the improvement in their quality, through increased public review, scrutiny and analysis. Worth noting, however, is the fact that higher standards of decisions may entail more effort and require more time and personnel in their production, which should be accounted for.

v. To provide access to precedents

In countries where the judicial decisions are a source of law (such as common law countries or some countries with civil law systems where judicial decisions have the force of judicial precedents or are officially recognised as such), easy and free access to them is of paramount importance.



18. *Drakšas v. Lithuania*, Application No. 36662/04, judgment of 31 July 2012, paragraph 61.

The objectives of automated jurisprudence retrieval systems are reflected in Recommendation No. R (95) 11 as follows:

- to facilitate the work of the legal profession by supplying rapid, complete and up-to-date information;
- to provide information for all persons directly or indirectly interested in a matter of jurisprudence;
- to make new judicial decisions available faster, especially in areas of law under development;
- to make available a larger number of judicial decisions concerning both questions of law and questions of fact (for example amount of compensation or of maintenance, length of a sentence, etc.);
- to contribute to the coherence of jurisprudence without introducing inflexibility;
- to enable law makers to analyse the application of laws;
- to facilitate research on jurisprudence;
- in certain cases, to furnish information for statistical purposes.

Thus, the publication of judicial decisions should be accompanied by a regulatory framework, setting out the goals and objectives of publication. This framework should be assessed regularly to check that the goals, objectives and other parameters set out have not lost their relevance and pertinence.

3. Policies

The definition of the goals, objectives, scope and methods of publication of "legal information", which includes all official texts of laws together with important judicial decisions, could be set out in specific policies. The list of main issues to be addressed in these policies is provided in Recommendation Rec(2001)3 and includes the following aspects: availability, accessibility, timeliness, accuracy, authenticity, copyright, responsibility, charging, privacy and transparency.

Availability	States should make the official texts of laws and important judicial decisions available to the public in readily accessible form electronically.
Accessibility	All legislation, including regulations, case law and parliamentary materials should be accessible to all.

Timeliness	To be effective, public legal information systems should be kept up to date and published quickly. Immediacy is vital for important court judgments, particularly for lawyers and the judiciary.
Accuracy	Rigorous quality supervision procedures should be put in place to ensure that texts published in electronic form are identical to the enacted texts or published judgments.
Authenticity	Authenticity of electronic texts should be guaranteed by appropriate means such as electronic/digital signature.
Copyright	While in most states there is no copyright on legal texts, there remains an obligation on the state to ensure that the texts remain correct. Where the official text is reproduced by private sector publishers, the source should be indicated, and the obligation for accuracy will rest with those private sector publishers.
Responsibility	Responsibility for the accuracy of electronic information should rest with the public publisher.
Charging	Access to legal database information should, in principle, be free of charge for all original legal texts.
Privacy	The issue of anonymity for parties in court judgments varies from one country to another and there may be a need to review the issue in a European context.
Transparency	To enable the easy use of the systems for the citizen, and to make the law readily understandable, the information systems should provide consolidated texts. States need to consider how these consolidated texts are accorded authoritative status.

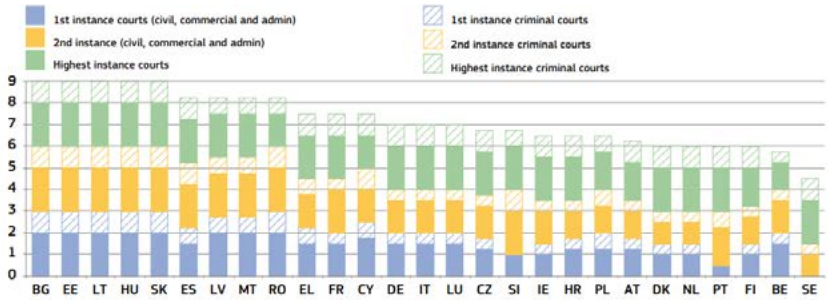
Recommendation Rec(2001)3 underlines that the formulation of such policies should aim for cohesive results that could be achieved through co-operation between national organisations, taking into account the wider European and global environment.

4. Scope of publication

The decision on the scope of publication is important. First, a decision should be taken about the necessity to publish the decisions of courts of first instance. In this regard, the role of first instance decisions in the interpretation of legal norms and formulation of approaches to new questions or new aspects of public life should be considered. In some member states, only the decisions that represent an important development of jurisprudence or are related to an important question are published. In this case, the next question for consideration would be who should take (and, if envisaged, approve) a decision about the publication. In some jurisdictions, the decision on the scope of publication is taken by the judge who prepared the decision. However, it may be practical for several judges to take a collegial decision on this question.

Online access to judgments is one of the indicators applied in the European Union Justice Scoreboard to measure the digitalisation of justice, which in turn is one of the means to increase transparency of the work of courts and facilitate access to justice. According to the 2023 European Union Justice Scoreboard,[19] almost all EU member states provide online access to judgments adopted by the courts of all three instances.

Online access to published judgments by the general public, 2022
(civil/commercial, administrative and criminal cases, all instances)
(source: European Commission)



19. European Union (2023).

The next question for consideration is whether the judicial decisions that are overturned at a higher instance should be published. Here, two approaches are possible.

The first approach is to have all decisions published. This would allow for a better understanding of the reasons for which some of them were overturned and the respective arguments of higher courts. This could have a positive effect if such reasons and arguments are taken into account by all judges. If this approach is chosen, there are three important aspects to consider:

1. the decisions that are overturned need to display clearly any relevant notes (annotations) so that they are not confusing to readers. Recommendation No. R (95) 11 proposes that when an appeal against a selected decision has been made to a higher court, users should be informed of the appeal whenever the decision is presented.
2. Such appealed or overturned decisions should be clearly linked to the decisions of the higher court to allow full analysis of the case in light of all relevant decisions by the respective courts.
3. It should be easy to navigate through the huge number of existing decisions, to make it possible to analyse the development of the judicial practice on particular matters. Navigation could be facilitated by categorisation, indexing and tagging of published cases (for more information see section 3 (ii) of Chapter IV).

The second approach is to publish only selected cases that represent an important or interesting development in domestic jurisprudence. However, such a selective approach may impact the transparency of judicial procedures and affect the quality of those judicial decisions which are not published.

Of course, the first approach (the publication of all decisions) should be selected by jurisdictions where court decisions have the binding force of judicial precedents.

In determining the appropriate scope of publication, one of the goals to consider is the provision of information to legal experts and the wider public on the development of jurisprudence, and of new legal rules that can be deduced from, in the main, final decisions. Consequently, the final character of judicial decisions to be published may be one of the criteria for consideration regarding the scope of publication. Following this, decisions that are overturned by higher courts have less interest for the public and their publication may even be confusing if the text is not clearly marked as having no legal force. At the same time, publication of overturned decisions may be of interest for legal

analysis of the reasons for the higher court's departure from the position of the lower court and the respective argumentation.

The following questions are examples of what can be considered and addressed in determining the scope of publication:

1. What judicial decisions should be published: level (first, second, third instance)?
2. Which type of decisions should be published (final/non-final)?
3. Which type of cases should be published (civil, criminal, administrative, labour, etc.)?
4. Should all decisions or only selected decisions be published?
5. Who will decide on the decisions to be published (for example the presiding judge or several judges (collegial decision))

The answers to these questions will also be relevant during the preparation of the anonymisation methodologies and tools discussed later in this report.

5. Authority in charge of publication

Decisions concerning publication and its scope lie in the hands of the institution that is competent for the judicial decision to be issued. Often, the same institution, which can be the ministry of justice, the Supreme Court, or court service (which is often an independent agency), performs both functions. Depending on which state institution takes such decisions, the scope of responsibility for eventual breaches related to personal data may be different. One example of this is in the application of the General Data Protection Regulation[20] (GDPR). As will be discussed below, courts, when acting in their judicial capacity, are excluded from having the competence of supervising authorities to monitor the application of the GDPR. This means that the possibility for the state authorities to regulate the publication of personal data by courts is minimal (if it exists at all). However, publication still represents a possible interference in the right to respect for private and family life as guaranteed by Article 8 of the Convention (for more details see section 3 of Chapter II). At the same time, when the authority for publication lies with the ministry of justice or a particular institution such as a court service, which are subject to the GDPR, then the supervising authority in charge of personal data protection can regulate the processing (including publication) of personal data, including in judicial decisions.

20. European Union (2016a).

Aside from legal issues of responsibility or liability, where the authority for publication lies can also have practical impacts, such as on the authenticity and consistency of published texts.

The publication of judicial decisions can be arranged by a number of entities, such as the state authorities or private organisations maintaining legal databases; sometimes such organisations are created and/or maintained by universities, lawyers associations, publishing houses, etc. When the publication is arranged by state authorities it can be undertaken either by judiciaries themselves or by the ministry of justice.

When the judiciary is not directly involved in the publication (and only transmits the texts for their further publication), there needs to be special arrangements in place for establishing co-ordination between the judiciary and the publishers. This helps to ensure the accuracy of the published text and, in particular, ensures that any amendments to the original text are reflected in the published version.

As raised above, determining whether courts are acting in their judicial capacity when in charge of publication and taking related decisions on the publication of personal data will have important implications for the protection of personal data.

The GDPR "applies, *inter alia*, to the activities of courts and other judicial authorities", and at the same time, advises that laws of the member state "could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities".[21] The GDPR is clear, however, that "[t]he competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity", and furthermore that "[i]t should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation". This safeguards the independence of the judiciary in the performance of its judicial tasks, including decision making. Article 55, paragraph 3, of the GDPR confirms this by stating that "[s]upervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity".

However, the exact extent of "acting in their judicial capacity" is still being determined. In a recent judgment of the Court of Justice of the European Union

21. European Union (2016a), General Data Protection Regulation, Recital 20.

("Court of Justice") in relation to the application of Article 55, paragraph 3, of the GDPR to the request for the preliminary rulings, the Court of Justice ruled that:

> [34] Article 55(3) of Regulation 2016/679 to processing operations carried out by courts 'acting in their judicial capacity' must be understood, in the context of that regulation, as not being limited to the processing of personal data carried out by courts in specific cases, but as referring, more broadly, to all processing operations carried out by courts in the course of their judicial activity, such that those processing operations whose supervision by the supervisory authority would be likely, whether directly or indirectly, to have an influence on the independence of their members or to weigh on their decisions are excluded from that authority's competence.
>
> [39] Article 55(3) of [the GDPR] must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data in order to enable them better to report on the course of those proceedings falls within the exercise, by that court, of its 'judicial capacity', within the meaning of that provision." [22]

22. Court of Justice case of 24 March 2022, *X and Z v. Autoriteit Persoonsgegevens*, C-245/20, ECLI:EU:C:2022:216, paragraphs 34 and 39.

Chapter 2

Personal data and the right to privacy

Data protection is a fundamental right[23] and an element of the right to respect for private life. It comprises not only standards in terms of processing and storing personal data, but also guarantees the right to be informed about and gain access to stored personal data, and to rectify and erase where there is no explicit legal basis for further storing or archiving personal data. Any judicial decision contains information about various individuals: parties to the case, their lawyers and representatives (if any), witnesses, experts, third parties involved and so on. This information represents the personal data of such individuals. Although there may be an indisputable interest in processing, storing and archiving personal data related to judicial proceedings, the disclosure of personal data through publication may cause irreversible damage and needs to be handled with due diligence.

This chapter provides an overview of the relevant international standards and considerations pertinent to the use and protection of personal data in publicly available judicial decisions. It examines how the long tradition of public trials and the need for transparency of justice has now intersected with new digital tools and online communications, resulting in new consequences, practicalities and challenges to address, the protection of personal data being chief among them.

23. GDPR, Recital 1; *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], Application No. 931/13, judgment of 27 June 2017, paragraph 137.

In particular, this chapter examines: the scope of and legal distinctions between categories of protected data under the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108")[24] and its protocols; the GDPR; the implications of requests to access personal data; and the balancing of interests between privacy rights and publication in the public interest that judiciaries will face. It also explores several practical and technical aspects in the context of data protection, such as the right to be forgotten and contextualises the discussion with references to approaches taken by the European Court.

1. Personal data

i. International regulation

The notion of personal data is set forth in national legislation, as well as in several international instruments, namely Convention 108 and its Additional Protocol related to supervisory authorities and transborder data flows.[25] Convention 108 was opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. Under this convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect for the fundamental human rights of all individuals with regard to the processing of personal data.

The core principles contained in Convention 108 and its technologically neutral, principle-based approach have made it a unique and valuable instrument. It is the only treaty that provides for a legally binding commitment of countries in the field of data protection with a global dimension and a fully horizontal scope of application (covering public and private sector processing). The convention was further modernised in 2018 ("Convention 108+")[26] to respond to new challenges in the digital era, allow safer exchanges of personal data at international level and strengthen the effective implementation of the convention.

24. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
25. Council of Europe Data Protection website, available at https://rm.coe.int/1680080626.
26. Convention 108+, available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

At the EU level, data protection is primarily regulated by the GDPR. It is directly applicable in EU member states, strengthening individuals' privacy rights and unifying rules for businesses in the processing of personal data.

ii. Definition

In general, "personal data" means any information relating to an identified or identifiable individual. An identifiable individual is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This definition therefore provides that "personal data" means information belonging to both an "identified" and an "identifiable person" who are accordingly "data subjects", namely persons whose data are processed.

It is settled case law of the Court of Justice that the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as "personal data".[27]

iii. Special categories of data

The term "special categories of data" refers to data that, due to their value to a person, require special treatment or more careful handling. The definition of these data may vary.

According to Article 6 of Convention 108, special categories of data are: genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures (as noted in the Explanatory Report to Convention 108+, these may refer to involving deprivation of liberty);[28] biometric data uniquely identifying a person; and personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health or sexual life.

The European Court has also found that certain types of data may require particular protection. In a case concerning the retention in a police database

27. Court of Justice case of 14 February 2019, *Sergejs Buivids v. Datu valst inspekcija,* C-345/17, ECLI: EU: 2019:122, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0345.
28. Council of Europe Treaty Series No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, paragraph 57, available at https://rm.coe.int/16808ac91a.

of data relating to a peaceful demonstrator, revealing his political opinions, such data was acknowledged to be sensitive.[29]

The GDPR contains a different list of special categories, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Under the GDPR, data related to criminal convictions and offences, or related security measures are not a special category; however, they may be processed only under specific circumstances. According to Article 10, processing is allowed if authorised by European Union or member state law providing for appropriate safeguards for the rights and freedoms of data subjects.

In general, the processing of data that fall under the notion of a special category entails additional requirements. For instance, legislation providing for the processing of personal data related to health should also provide additional safeguards.

2. Scope of regulation

Convention 108 gives to its member states a margin of appreciation when restricting the application of certain of its provisions when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

i. the protection of national security, defence, public safety, important economic and financial interests of the state;

ii. the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties; and

iii. other essential objectives of general public interest.

However, such exceptions or restrictions cannot apply to standards set by Convention 108 regarding the legitimacy of data processing, data security, transparency of processing or the rights of data subjects.

29. *Catt v. the United Kingdom*, Application No. 43514/15, judgment of 24 January 2019, paragraph 112.

At the level of the European Union, the GDPR is not applicable to data processing in connection with the fight against crime or public safety, nor the matter of national security. The former is regulated under the Law Enforcement Directive[30] (LED) adopted together with the GDPR.[31] As seen in Chapter I, the GDPR is applicable to the activities of courts and other judicial authorities, however, national law could specify the processing operations and procedures concerning the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision making (for more information see section 0 of Chapter I above). Supervision of data processing operations could be entrusted to specific bodies within the judicial system of the member state, which should, in particular, ensure compliance with the rules of the GDPR.[32]

3. Right to respect for private and family life (Article 8 of the Convention)

The right to personal data protection forms part of the right to respect for private life, home and correspondence under Article 8 of the Convention. As the European Court has held that it is established case law that the release or use by a public authority of information relating to a person's private life amounts to an interference with Article 8 paragraph 1, of the Convention.[33]

Any interference with the rights protected by Article 8, paragraph 1, must fulfil all of the criteria listed in Article 8, paragraph 2, in order to be consistent with the Convention.

30. European Union (2016b).
31. The Law Enforcement Directive took effect in May 2018 in parallel to the GDPR. The LED concerns the processing of personal data by data controllers for law enforcement purposes and falls outside of the scope of the GDPR.
32. European Union (2016a), GDPR, Article 55; Recital 20.
33. *Leander v. Sweden,* Application No. 9248/81, judgment of 26 March 1987, paragraph 48, and *Rotaru v. Romania*, Application No. 28341/95, judgment of 4 May 2000, paragraph 46, *L.B. v. Hungary*, Application No. 36345/16, judgment of 9 March 2023, paragraph 42.

Article 8, paragraph 2, of the Convention

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Both the European Court and the Court of Justice have specified that a balancing exercise with other rights is necessary when applying and interpreting Article 8 of the Convention and Article 7 of the Charter of Fundamental Rights of the European Union[34] (respect for private and family life). Any exemptions from and restrictions to the right to privacy "may be provided for at national level; they must be provided for by law, pursue a legitimate aim and be necessary in a democratic society".[35]

According to Recommendation No. R (95) 11, where issues of privacy and protection of personal data arise in computerised legal information systems, they should be regulated by domestic law in accordance with the principles laid down by Convention 108. Therefore, a national legal framework regulating the protection of personal data in relation to the publication of judicial decisions needs to be in place.

Personal data protection in the context of the publication of national court decisions has been addressed in a number of judgments of the European Court (under Article 8 of the Convention).

Data protection – Guide to the case law of the European Court

Paragraph 244. In order to determine, in any given case, whether there are sufficient grounds for disclosing, in the body of a judicial decision, the identity of an individual and other personal data on the latter, one important question is whether other less intrusive measures would have been possible under domestic law and practice. This includes the possibility of a court omitting mentioning any names in the judgment permitting the identification of the data subject (*Z v. Finland*, 1997, paragraph 113; *Vicent Del Campo v. Spain*, 2018, paragraph 50), keeping the full reasoning

34. European Union (2012).
35. EU FRA (2018).

confidential for a certain period and instead publishing an abridged version of the reasoning, the operative part and an indication of the law which it had applied (*Z v. Finland*, 1997, paragraph 113), or restricting access to the text of a judgment or to certain matters therein (*Vicent Del Campo v. Spain*, 2018, paragraph 50). The Court considers that such measures are generally deemed capable of reducing the impact of a judgment on the data subject's right to protection of his private life.

An illustrative case examined by the European Court on the topic of personal data disclosure in published judicial decisions is *Vicent Del Campo v. Spain*.[36]

Vicent Del Campo v. Spain

This case concerns a violation of the applicant's right to respect for his private life due to the fact that he had been identified by his name in a domestic court decision issued in 2011 at the end of proceedings to which he was not a party, amounted to a violation of Article 8.

The judgment of the High Court of Justice had disclosed the applicant's identity, finding that his conduct had amounted to psychological harassment and bullying, although the actual defendant in the case was his local authority employer. Holding that the publication of those findings had been capable of adversely affecting his enjoyment of private and family life, the Court considered that the complaint fell within the scope of Article 8. Also, the Court considered that the disclosure of the applicant's identity in the reasoning of the judgment of the High Court of Justice could not be considered to be a foreseeable consequence of the applicant's own doing.

The applicant had not been informed, questioned, summoned or in any other way notified of his colleague's complaint pending before the High Court of Justice. Accordingly, he had not had the opportunity to request the non-disclosure of his identity or personal information by the High Court of Justice before its judgment was passed. The interference with the applicant's private life had thus not been accompanied by effective and adequate safeguards.

Accordingly, following the reasoning of the European Court, the measures complained of had constituted an "interference" with the applicant's right to respect for his private life and pursued the aim of "the protection of the rights and freedoms of others".

36. *Vicent Del Campo v. Spain*, Application No. 25527/13, judgment of 6 November 2018.

The case *L.B v. Hungary*[37] is another illustrative example of the importance of developing a regulatory framework for the online publication of judicial decisions that provides a basis for balancing of individual rights and the public interest and related remedies.

L.B v. Hungary

This case is about the online publication of personal data (including the home address) of a debtor taxpayer by the tax service. National legislation provided for the systematic and mandatory publication of major tax debtors' personal data (as a general measure), without any discretion given to the tax authorities to review the necessity of publishing taxpayers' personal data to weigh-up the competing individual and public interests. In that context the quality of the parliamentary review of the necessity of the interference was of central importance in assessing the proportionality of a general measure.

The balancing (weighing-up) of the individual and public interests should be possible either at the level of the application of the regulation, or when it is being adopted. The existence of procedural safeguards might also play an important role. The following five aspects are important for this balancing exercise:

1. the public interest in dissemination of the information in question;
2. the nature of the disclosed information;
3. the repercussions on and risks for the private life of the persons concerned;
4. the potential reach of the medium used for the dissemination of the information in particular, that of the internet;
5. the basic data protection principles (including those on purpose limitation, storage limitation, data minimisation and data accuracy).

37. *L.B. v. Hungary*, Application No. 36345/16, judgment of 9 March 2023.

4. Archiving, data retention and the right to be forgotten

i. The right to be forgotten

The right to be forgotten is the right to have private information about a person removed from internet searches and other directories under some circumstances. It may be relevant in the context of the publication of judicial decisions as the published decisions will be searchable in case-law databases and through other relevant directories long after initial publication.

Prior to the adoption of the GDPR, a Court of Justice decision in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*[38] articulated the right to be forgotten as the right of a data subject to go beyond the mere deletion of their personal data and request the removal of that data from other sources, such as search engine results.

The case in question, before reaching the Court of Justice, started in Spain, when Mr González addressed the Spanish Data Protection Agency asking for a removal of his personal data from an article in an online newspaper, as well as the concealing or removal of his personal data from search results on Google linking to that article. The agency rejected the complaint against the online newspaper as the information published was determined to be lawful and accurate, but accepted the complaint against Google. Google appealed the agency's decision before the Spanish High Court, who requested a preliminary ruling from the Court of Justice.

The Court of Justice held that a search engine could be obliged to remove links to web pages published by third parties and containing information relating to a person from search results on the basis of that person's name. This also applies in an instance where that name or information is not erased beforehand or simultaneously from those web pages, and even when its publication on those pages is lawful. The right of the data subject to demand such a removal is not dependent on the information concerned being prejudicial to them, as their fundamental rights to private life and protection of personal data outweigh the economic interest of the search engine operator and the interest of the general public in accessing such information.

It is worth noting that the Court of Justice did not extend this finding to all scenarios, noting that in cases involving a public figure, the interference with

38. Court of Justice case of 13 May 2014, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317.

their fundamental rights may be justified by the public interest in accessing the information in question.

The European Court has also dealt with the issue of the right to deletion of personal data ("the right to be forgotten") after a specific period of time in cases concerning the following topics:

- removal, after a certain lapse of time, of personal data (DNA profile, identity photographs and fingerprints) of individuals accused, or merely suspected, of committing an offence, that was collected by the authorities in databases aimed at preventing and fighting crime.[39]

Data protection – Guide to the case law of the European Court

Paragraph 293. In *Ayçaguer v. France*[40] the Court found a violation of Article 8 because, owing to its duration and the impossibility of deletion, the current regulations on the storage of DNA profiles in the national database, to which the applicant had objected by refusing to undergo sampling, did not provide the data subject with sufficient protection ... The Court emphasised that convicted persons should, like persons who were suspected of committing a criminal offence, discharged or acquitted, be given a concrete opportunity to submit a request for the deletion of stored data, so as to ensure that the period of data retention is proportionate to the nature of the offences and the aims of the restrictions (… *B.B. v. France*, 2009, paragraph 68; *Brunet v. France*, 2014, paragraphs 41-43[41]).

- removal, after a specific period of time, of police records about previous convictions.[42]

Data protection – Guide to the case law of the European Court

Paragraph 288. In *M.M. v. the United Kingdom*,[43] the lifelong registration of a caution in a person's police record led to a finding of a violation of Article 8. The Court considered that a conviction or a caution issued to an individual

39. *B.B. v. France*, Application No. 5335/06, judgment of 17 December 2009; *Gardel v. France*, Application No. 16428/05, judgment of 17 December 2009; *M.B. v. France*, Application No. 22115/06, judgment of 17 December 2009.
40. *Ayçaguer v. France*, Application No. 8806/12, judgment of 22 June 2017, paragraph 44.
41. 41. *Brunet v. France*, 2014, paragraphs 41-43.
42. *M.M. v. the United Kingdom*, Application No. 24029/07, judgment of 13 November 2012.
43. Ibid., paragraphs187-207.

in the past became, with the passage of time, an integral part of his or her private life, which had to be respected. Even though the data on the criminal record was, in a sense, public information, its systematic storage in central files meant that it could be disclosed long after the event, when everyone except the data subject would probably have forgotten the incident. The Court deemed disquieting the fact that the criteria for review to enable the data to be deleted had been very restrictive, and that requests for deletion were allowed only in exceptional cases.

- retention in the security service archives of individuals' personal data, which no longer complied with the requirement of being "necessary in a democratic society" in view of their nature and age.[44]

Data protection – Guide to the case law of the European Court

Paragraph 295. In the case of *Segerstedt-Wiberg and Others v. Sweden,*[45] the storage in the files of the State security services of very old personal data relating to the applicants' attendance at a political meeting, the fact that they had advocated violent resistance to police checks during demonstrations, and their membership of a specified political party, had amounted to a violation of Article 8. The Court considered that the State's interest in protecting national security and fighting terrorism, justifying the collection and storage of the information in question, should be balanced against the seriousness of the interference in the exercise by each of the applicants of their right to respect for their private life. In view of the nature and age of the information on the applicants, the reasons behind its storage, although relevant, could not be deemed sufficient 30 years later.

- Anonymisation of the online archived version of a lawful article published 20 years earlier, on the grounds of the "right to be forgotten".[46] The case *Hurbain v. Belgium* represented an important development of the Court's case law related to the right to be forgotten, in which the Court examined the criteria for balancing the right to be forgotten and the maintenance of integrity of online archives.

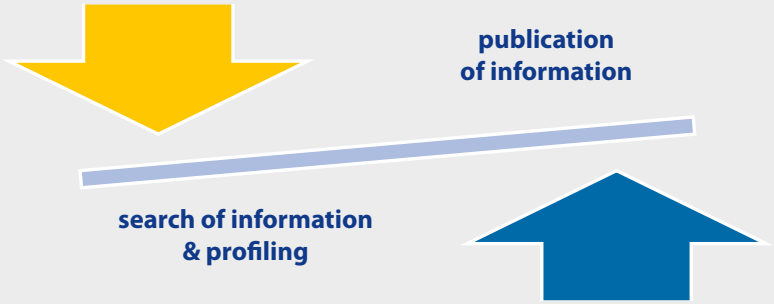
44. *Segerstedt-Wiberg and Others v. Sweden*, Application No.62332/00, judgment of 6 June 2006.
45. Ibid., paragraphs 73-92.
46. *Hurbain v. Belgium*, Application No. 57292/16, judgment of 4 July 2023.

Hurbain v. Belgium

In this case a newspaper publisher (Mr Hurbain) was ordered in a civil judgment to anonymise, on grounds of the "right to be forgotten", the electronic archived version of an article originally published in 1994 in the newspaper's print edition and placed online in 2008. The article mentioned the full name of G., the driver responsible for a fatal road-traffic accident.

In its Grand Chamber judgment of 4 July 2023, the European Court found no violation of the Convention (namely freedom of expression and press freedom) in the actions of the Belgian courts, which ordered the anonymisation of the article.

The balancing of the interests at stake (freedom of the press versus the right to privacy, which are both of equal value) may result in different outcomes depending on whether a request for deletion concerns i. the original publisher of the information (especially a publishing house which enjoys protection of the freedom of expression), or ii. a search engine whose main interest is not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her.



This case concerned solely the continued availability of the information on the internet rather than its original publication. The original article had been published in a lawful and non-defamatory manner. In order for Article 8 of the Convention to come into play, an attack on a person's reputation stemming from the continued online availability of an archived article had to attain a certain level of seriousness, which had to be duly substantiated by the person making such a request.

The "right to be forgotten" was based on the interest of an individual who was the subject of an online article in obtaining the erasure or alteration of, or the limitation of access to, past information that might have a far-reaching negative impact on how he or she was currently perceived by public opinion. There were such potential negative risks as: i. creation of a profile of the person concerned; ii. an individual consulting an online article about another individual received a fragmented and distorted picture of the reality if the information was not placed in context; iii. fear for that person to be unexpectedly confronted with his or her past actions at any time and in a variety of contexts such as, for instance, job-seeking and business relations.

The "right to be forgotten" first emerged in the context of the republication by the press of previously disclosed information of a judicial nature. In the context of the digitisation of news articles this results in their widespread dissemination on various websites. The effect of this dissemination is magnified by the listing of websites by search engines. In such cases the issue is not the resurfacing of the information but rather its continued availability online.

The following general principles formulated in the case law of the Court were reiterated in this case.

1. States have greater margin of appreciation in striking the balance between competing rights (in this case freedom of expression on the one side and the right to privacy on the other) in relation to publication of past events. The duty of the press to respect the principles of responsible journalism by ensuring the accuracy of historical information published is more stringent when there is no urgency in publishing the material.
2. The role of archives is to ensure the continued availability of information that was published lawfully at a certain point in time. The archives should, as a general rule, remain authentic, reliable and complete. Accordingly, the integrity of digital press archives should be the guiding principle underlying the examination of any request for the removal or alteration of all or part of an archived article which contributes to the preservation of memory. The removal of archived content should be limited to what is strictly necessary.

In its analysis in the present case, the Court considered that the following criteria should be taken into account in each case of a request to alter journalistic content that is archived online.

a. Nature of the archived information

Does the information related to the private, professional or public life of the person concerned have a social impact?

Does it fall within the intimate sphere of private life and is therefore particularly sensitive? In its recent case law, the Court has characterised data relating to criminal proceedings as sensitive.

b. Time elapsing since the events and since the initial and online publication

In this case 16 years had elapsed between the initial publication of the article and the first request for anonymisation. In those circumstances, G., who had been rehabilitated, the Court decided that G. had a legitimate interest, after all that time, in seeking to be allowed to reintegrate into society without being permanently reminded of his past.

c. Contemporary interest of the information

Does the article in question continue to contribute to a debate of public interest? Has it acquired any historical, research-related or statistical interest? Does it remain relevant for the purposes of placing recent events in context in order to understand them better?

An article's contribution to a debate of public interest might persist over time (either because of the information itself or because of new factors arising since publication). However, due to their specific nature, digital press archives rarely contain information that is of topical relevance (contributing to a contemporary debate of public interest).

Is the archived information of interest for any other (historical or scientific) purpose?

Is the original, non-anonymised, version of the article still available in print form and could it therefore be consulted by any interested person, thus fulfilling its inherent role as an archive record?

d. Whether the person claiming entitlement to be forgotten is well known, and his or her conduct since the events

The person's conduct since the events that were the subject of the original article might also justify refusing a "right to be forgotten" request in some situations. Conversely, the fact of staying out of the media spotlight might weigh in favour of protecting a person's reputation.

The case of G., an individual who was unknown to the public and had not sought the limelight, had not attracted widespread publicity either at the time of the events reported on or when the archived version of the article had been placed online.

e. Negative effects of the continued availability of the information online

In order to justify the alteration of an article stored in a digital press archive, the person concerned has to be able to make a duly substantiated claim of serious harm to his or her private life. With regard to judicial information, it is important to assess the damage to the person concerned and consequences of the availability of the information for that person's reintegration into society.

Has the person's conviction been removed from the criminal records and has he or she had been rehabilitated? Individuals who have been convicted could legitimately aspire to being fully reintegrated into society once their sentence has been served. However, the fact of being rehabilitated cannot directly justify recognising a "right to be forgotten".

f. The degree of accessibility of the information in the digital archive

The degree of accessibility of the archived article is important: whether it is available without restrictions and free of charge or whether access is confined to subscribers or otherwise restricted.

In this case, the Court took into account that, in the absence of an active search (using keywords), an article contained in the digital archives was not, as such, likely to attract the attention of internet users who were not looking for precise information concerning a particular person.

g. The impact of the measure on freedom of expression and more specifically on freedom of the press

In determining disputes of this kind national authorities should decide which of the different measures are i. best suited to the aim pursued and ii. least restrictive of press freedom.

There is a whole range of available measures, for instance: a. reorganisation of the search results so that the link to the website in question appeared in a less prominent position in the list of results, or b. complete or partial delisting (relating only to searches based on the name of the person concerned) through the removal of the link from the search engine's index. The publisher

of a website could also, for instance: a. remove all or part of a text stored in the digital archive; b. anonymise the details of the person referred to in the text; c. add a notice to the text, that is, update the text by means of digital rectification (where the information was inaccurate) or via an electronic communication (where the information was incomplete); d. remove the article from the index of the website's internal search engine; or e. have the article de-indexed, either fully or partially (in relation only to searches based on the name of the person concerned), by external search engines, on the basis of access codes or directives issued to the search engine operators preventing their search programmes from crawling certain locations.

In this case the following measures were analysed to give effect to the "right to be forgotten": "delisting" – measures taken by search engine operators; and "de-indexing" – measures put in place by the news publisher responsible for the website on which the article in question was archived.

The national court took into consideration that 20 years had passed since the events; they were clearly not of historical significance; the person was not a public figure; and the publication did not add to the public interest, but merely made a statistical contribution to a public debate on road safety. The national court also considered that the presence of the article in the online archives was liable to stigmatise G., who was a doctor, and to seriously damage his reputation in the eyes of his patients and colleagues in particular and prevent him from reintegrating into society normally. On the basis of these arguments the national court ordered the anonymisation of the article in question.

Taking into account the careful balance of the rights at stake by the national courts in accordance with the requirements of the Convention, the Court decided that the interference with the right guaranteed by Article 10 had been limited to what was strictly necessary and could thus, in the circumstances of the case, be regarded as necessary in a democratic society and proportionate.

The Court held that anonymisation was less detrimental to freedom of expression than the removal of an entire article. The obligation for a publisher to anonymise an article that had been published initially in a lawful manner might in principle fall within the "duties and responsibilities" of the press and the limits which could be imposed on it. In the present case, it did not appear from the file that the anonymisation order had had a real impact on the performance by the newspaper of its journalistic tasks.

The right to be forgotten and time limitations on the retention of data can be important factors that judicial entities should consider in their decisions on publication and in the design of case-law management systems or other relevant information services, especially when third parties are involved in the publication or storage of the data.

ii. Length of personal data retention

The length of personal data retention can, among other things, be a determining factor in finding a violation of the rights to private life and data protection, and has been considered by the European Court in several cases. While these cases do not directly involve judicial publication, they contain important factors and delimitations that may be relevant to the processing and publication of personal data in judicial decisions.

The European Court has found that indefinite periods of retention can lead to a violation of Article 8 in the following cases.

- indefinite storage of fingerprints of and DNA data on individuals who were suspected of an offence but whose proceedings had ended with a discontinuance decision or an acquittal.

Data protection – Guide to the case law of the European Court

Paragraph 200. In *S. and Marper v. the United Kingdom* [GC], 2008 (paragraphs 119, 125),[47] a database in which it was possible to collect and store fingerprints, biological samples and DNA profiles from anyone suspected but not convicted of criminal offences, whatever their age, the nature and seriousness of the offences, without a time limit or any independent review of the justification of the retention of data according to defined criteria, had led to a finding of a violation of Article 8. The blanket and indiscriminate nature of such a system failed to reflect a fair balance between the competing public and private interests.

indefinite storage of the DNA profiles, fingerprints and photographs of an individual found guilty of an offence, even after their conviction had been deleted from their police record on expiry of the legal time limit.

47. *S. and Marper v. the United Kingdom* [GC], 2008, paragraphs 119, 125.

Data protection – Guide to the case law of the European Court

Paragraph 209. In the case of *Gaughran v. the United Kingdom*, 2020 (paragraph 96),[48] the indefinite nature of the storage of the fingerprints, DNA profiles and photograph of an individual found guilty of driving with excess alcohol had led to a finding of a violation of Article 8. The authorities had not had regard to the seriousness of the offence committed or to the continuing need to retain the said data indefinitely, nor had they provided any real review facilities.

- lifelong retention on a police record of all the convictions, acquittals, cautions, warnings and reprimands pertaining to one individual.

Data protection – Guide to the case law of the European Court

Paragraph 202. In the case of *M.M. v. the United Kingdom*, 2012 (paragraphs 187-207),[49] the lifelong entry of a caution in the police records of a person after she had gone missing for a day with her grandson, a baby, hoping to prevent his departure for Australia following the breakdown of her son's marriage, had led to a finding of a violation of Article 8. The Court called into question the extremely extensive scope of the data retention system, which covered not only convictions but also non-conviction decisions such as warnings, cautions and reprimands, as well as a large amount of supplementary data recorded by the police by virtue of a general guideline to the effect that data should be retained until the data subject had reached the age of 100.

When the period of data retention is defined, the European Court considers the following elements when deciding whether the defined period violates Article 8: i. the length of data retention period; ii. the serious of the offence; and iii. the possibility to review the term of the retention. Some examples of where the European Court has found violations include:

- retention for a maximum of 40 years, and the lack of the possibility of deletion, of the personal data of an individual convicted of a fairly minor offence (*Ayçaguer v. France*, 2017);[50]

48. *Gaughran v. the United Kingdom*, 2020, paragraph 96.
49. *M.M. v. the United Kingdom*, 2012 (paragraphs 187-207).
50. *Ayçaguer v. France,* Application No. 8806/12, judgment of 22 June 2017.

- retention for a maximum of 25 years, with an ineffective safeguard enabling a request for deletion, thus rendering this period the norm, of the fingerprints of an individual suspected, but not convicted, of stealing books (*M.K. v. France*, 2013);[51]
- retention for a maximum of 20 years, which in this scenario would be the norm, and with no real possibility of deletion, of the personal data of an individual following a complaint of violence against their partner, where the case was discontinued following mediation (*Brunet v. France*, 2014).[52]

Data protection – Guide to the case law of the European Court

Paragraph 210. A maximum storage period for personal data laid down in domestic law may be more akin, in practice, to a norm than to a real maximum if the chances of acceptance of a request for deletion of the data before expiry of the period laid down by law are merely hypothetical (*M.K. v. France*, 2013, paragraphs 44-47; *Brunet v. France*, 2014, paragraphs 41-45; *Ayçaguer v. France*, 2017, paragraphs 44-46). The Court has found a violation of Article 8 in several cases where the national system provided for maximum periods of storage of 20 or 25 years for offences in which proceedings had been discontinued (*M.K. v. France*, 2013, paragraphs 44-47; *Brunet v. France*, 2014, paragraphs 41-45), and indeed a maximum forty-year storage period in the case of an offence that had not been particularly serious but which had led to a conviction (*Ayçaguer v. France*, 2017, paragraph 42).

In several cases the European Court has found no violation.

Data protection – Guide to the case law of the European Court

Paragraph 205. Conversely, the Court found no violation of Article 8 in several cases concerning the storage of the personal data of individuals convicted of sexual assault for a maximum 30 years, after which period the data was automatically deleted, because procedures had been introduced to enable the data to be deleted as soon as it was no longer relevant (*B.B. v. France*, 2009, paragraph 67; *Gardel v. France*, 2009, paragraph 69; *M.B. v. France*, 2009, paragraph 59) ….

51. *M.K. v. France*, Application No. 19522/09, judgment of 18 April 2013.
52. *Brunet v. France*, Application No. 21010/10, judgment of 18 September 2014.

In the case of *P.N. v. Germany*, 2020 (paragraphs 87-90), the Court found no violation of Article 8 with regard to the retention for five years, subject to guarantees and individualised review, of a repeat offender's personal data for the purposes of identifying him following the commencement of fresh criminal proceedings against him.

The European Court has also considered the situation where there is no defined maximum period, or an indefinite period, of data retention.

Paragraph 207. The lack of a maximum period for the retention of personal data is not necessarily incompatible with Article 8 (*Peruzzo and Martens v. Germany* (dec.), 2013, paragraph 46; *Gaughran v. the United Kingdom*, 2020, paragraph 88), but procedural safeguards are especially necessary where the storing of the data depends entirely on the diligence with which the authorities ensure the proportionality of the data retention period (*Peruzzo and Martens v. Germany* (dec.), 2013, paragraph 46; *Ayçaguer v. France*, 2017, paragraph 38).

These limits and requirements on data retention can raise important considerations for the processing and publication of personal data in judicial decisions.

With regard to criminal proceedings and the public's interest in them, the Court of Justice considered that personal data processing may become no longer necessary in relation to the purpose for which such data was collected. With the passage of time, the information may turn out to be inadequate, irrelevant or excessive. With reference to the European Court judgment in case *M.L. and W.W. v. Germany*,[53] the Court of Justice noted (in relation to reporting in some press articles on the opening of an investigation, but not on its subsequent closure) that the operator of a search engine should adjust the list of results to ensure that the overall picture given reflects the current legal position.[54]

53. *M.L. and W.W. v. Germany*, Application Nos. 60798/10 and 65599/10, judgment of 28 June 2018.
54. Court of Justice case of 10 January 2019, *G.C. and Others v. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, ECLI:EU:C:2019:773.

Consequently, following on from the reasoning given in the cases above, it could be argued that personal data in criminal convictions may not be stored indefinitely or for an extended period in case-law databases. This may apply even to cases with pseudonymised texts, since the possibility of re-identification cannot be excluded. To mitigate these concerns, it could be proposed that the state authorities in charge of the information stored in the CMSs and case-law databases ensure that the texts are anonymised after a certain period (namely that the personal data is deleted without any possibility of re-identification of data subjects).

iii. Archiving

Considering the essential role of archiving as part of case processing in the legal/judicial sector, a number of practical recommendations have been provided in the Committee of Ministers Recommendation Rec(2003)15 on archiving of electronic documents in the legal sector:[55]

- all operations concerning the archiving of electronic documents should be subject to procedures ensuring their traceability.
- the entry, modification or deletion of electronic documents in electronic document archiving systems should be undertaken by specialists authorised and trained to carry out such operations.
- procedures should be put in place to ensure the physical protection of premises where the electronic document archiving systems are situated, including adequate storage conditions and access control.
- the electronic document archiving systems should be subject to periodic assessment.

Ensuring the uniformity of document formats used in the legal sector is another important recommendation, especially in situations where judicial decisions are produced by different courts in different formats. Recommendation Rec(2003)15 also advises member states to ensure that these formats are open, international and standard, and that they permit subsequent migration of data and allow processing in different languages.

55. Committee of Ministers (2003b).

Chapter 3

Anonymisation/ pseudonymisation

Anonymisation and pseudonymisation represent two practices that may reconcile privacy and data protection rights with the need for public access to judicial decisions and the transparency of judicial procedures.

This chapter examines the definitions and practicalities of anonymisation and pseudonymisation, highlighting both challenges to their implementation and potential solutions. It delves into specific methodologies (such as *ex ante* and *ex post* anonymisation) and the scope of their functionality, examining questions such as where in the case life cycle to implement anonymisation/pseudonymisation, internal versus external systems and the level of control and human feedback necessary in the process.

This chapter further explores how anonymisation/pseudonymisation represents an accommodation between the public interest in transparency and the privacy of parties. However, within this compromise, considerations arise about preserving the legal essence of decisions and their comprehensibility while ensuring adequate privacy. This can be difficult, both on a technical level, in terms of using adequate resources and tools to deliver the desired result, and on a procedural level, where there is a need to ensure that the decision-making judicial body has sufficient authority to assess the extent of the anonymisation/pseudonymisation to be performed.

Furthermore, this chapter raises some further specific challenges arising from the publication of judicial decisions that will affect the design and administration of the tools and solutions used for anonymisation/pseudonymisation.

1. General considerations on anonymisation approaches

The online publication of judicial decisions requires balancing the right to data protection and the publication of judicial decisions to ensure the transparency of justice systems. This question of balance was addressed in 1983 in the Committee of Ministers Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics,[56] which specifically recommends that whenever possible, research should be undertaken with anonymous data. Scientific and professional organisations, as well as public authorities, should promote the development of techniques and procedures securing anonymity. Two such techniques are pseudonymisation and anonymisation.

Pseudonymisation is a data security measure used either when required by legislation, for example in the case of clinical trials, or as an additional measure to prevent risks to data subjects.

Pseudonymous data are data that cannot be attributed to a specific individual (in data protection terminology: a data subject) without the use of additional information held for the purpose of identifying a data subject. This additional information is kept separately.

In the case of pseudonymous data, the data subject is unknown to all those that cannot use or access the additional information. However, even though the data subject is unidentifiable to the public, re-identification is still possible and the pseudonymous data are therefore considered to be personal data, thus falling under the data protection regime.

Unlike pseudonymous data, anonymous data means that personal data referring to a data subject can no longer be used to identify that subject. In other words, re-identification is impossible. Since anonymous data cannot be attributed to a specific data subject, they are not considered to be personal data and therefore the data protection regime does not apply.

However, it should be noted that truly irreversible anonymisation may be considered to be impossible, bearing in mind the wide scope of personal data that can be used to identify a subject on the one hand, and the power of technology on the other.

When considering these techniques in relation to the publication of judicial decisions, pseudonymisation not only applies to personal data directly linked

56. Committee of Ministers (1983b).

to the parties or accused (names, dates of birth or addresses), but also to indirect information from which the reader can draw conclusions and identify a person by putting several pieces together (professions, property or other unique characteristics). While the first category of data is relatively easy to detect and process, indirect information requires much deeper knowledge of the case concerned.

Pseudonymisation usually represents a compromise between the public interest in transparency and the privacy of persons involved in the proceedings. Decisions served to the parties, in general, will not require anonymisation/pseudonymisation at all, since the parties are participants in the proceedings and have full and private access to the court files. Thus, anonymisation/pseudonymisation is mainly an issue in cases of the disclosure of decisions to the public, in particular, when effected by means of the internet and automated data processing.

2. Legal regulation of anonymisation/pseudonymisation

The purpose of anonymisation/pseudonymisation may seem contradictory to the transparency goals of publication but it is necessary to secure the positions and rights of the parties to or other participants in the proceedings. Whether or not these groups are entitled to the anonymisation/pseudonymisation of their personal data relies on a fair balance of interests, which should be performed through setting up a special legal framework.

In its Recommendation No. R (95) 11, the Committee of Ministers indicated that where issues of privacy and protection of personal data may arise in computerised legal information systems, they should be regulated by domestic law in accordance with the principles laid down by Convention 108 and its subsidiary texts.

When legal regulation is absent, one could argue that an interference in privacy rights in the form of the publication of personal data is not in accordance with the law. The respective legal regulation should, in particular, provide for the goals of anonymisation/pseudonymisation, taking into consideration the risks related to the open publication of personal data.

The case of *Mitov and Others v. Bulgaria*[57] provides an illustrative example of national regulation of access to judicial information and personal data

57. *Mitov and Others v. Bulgaria*, Application No. 80857/17, decision of 28 February 2023.

protection. The respective complaint on the restriction of the freedom to access the information was rejected by the European Court as there is no abstract right to have unlimited access to judicial decisions through online databases.

Mitov and Others v. Bulgaria

This case concerned access by journalists to materials of administrative cases in the Supreme Administrative Court's online database.

The applicants, journalists from various Bulgarian media specialising in reporting on matters relating to the domestic judicial system and a non-governmental organisation, complained under Article 10 (freedom of expression and access to information) about two matters:

1. the September 2016 anonymisation rules adopted by the Supreme Administrative Court that removed online access to scanned case material previously available in unredacted form and introduced anonymisation (redaction of all personal data) of decisions and other case material published in that court's online database;
2. the November 2017 statutory amendment under which final decisions in criminal cases which convicted and sentenced someone or finally upheld convictions and sentences would only be published on the relevant court's website after steps had been taken to enforce them.

The complaints did not contain the necessary elements of the right to access to information. These elements (four criteria for the right of access to State-held information) were developed in the case of *Magyar Helsinki Bizottsg v. Hungary GC*[58]:

1. the purpose of the information request;
2. the nature of the information sought;
3. the role of the seeker of the information in receiving and imparting it;
4. whether the information is ready and available.

The applicants did not complain about a specific piece or even a defined category of information held by a public authority, but about the impossibility of accessing on the internet all scanned case material available in the Supreme Administrative Court's database and the anonymised parts of all that courts judgments and decisions. With regard to the deferred-publication

58. *Magyar Helsinki Bizottság v. Hungary*, Application No. 18030/11, judgment of 8 November 2016.

rule for criminal cases, the Court reiterated that it is impossible to assess in the abstract whether that provision will actually hinder the applicants' reporting on matters of public interest. Although the applicants' role as "public watchdogs" was not in doubt, their argument that all information relating to cases concerned matters of public interest and that the impossibility of or delays in accessing it hindered them from reporting on such matters was entirely abstract.

The Court could not conclude that the information to which the applicants claimed not to have access was instrumental for the exercise of their right to freedom of expression, and therefore rejected the application as inadmissible.

3. Methodologies for anonymisation/pseudonymisation

There are different models of anonymisation of judicial decisions; from the entirely automated (based on predefined specific text templates), to semi-automated (utilising text recognition and marking it for human review and decision), to those handled entirely manually by judges' assistants or other designated court staff.

In the present context, it is important to consider the line drawn between *ex ante* and *ex post* anonymisation/pseudonymisation, that is to say, the moment when the editorial decision on the protected content leaves the control of the decision-making body or persons and changes to the editorial decision are no longer possible.

The advantage of an *ex ante* approach is that the decision-making body is fully aware of the process of anonymisation, leaving enough space for adaptations while drafting and letting the specific decisions remain within the control of the decision-making body or institution. This applies not only to conventional, human-administered processes, but also to machine-based support, which can be organised as a real-time assistant – intervening in the drafting phase by tagging protection-sensitive content and offering proposals for anonymisation/pseudonymisation – or as a review tool after the drafting process is finished. When combined with a robust methodological approach based on draft guidelines or respective training of judicial staff, whether on the requirements of anonymisation/pseudonymisation in the light of data protection, or on the functioning of the machine-based anonymisation tool, optimal results can be expected. Although this process may represent an additional burden on judicial staff to begin with, once trained, the results and efficiency of the tool may be enhanced over time.

On the other hand, the *ex post* approach promotes the standardisation of anonymisation/pseudonymisation processes, applying the editorial decisions on identifying and removing protected data later in the publication cycle, and avoiding the decision-making bodies' case-by-case basis and involvement. One advantage of this approach is that the decision-making bodies (that is to say, the judges and judicial or court staff) may save time and focus on dealing with core legal questions rather than struggling with what are basically procedural questions, unrelated to the adjudication of the case before them. However, a mixed approach employing an initial *ex post* process but with a feedback loop that includes the approval by the judicial body of the final draft may be a more optimal method.

At present, the accuracy of fully automated anonymisation/pseudonymisation without human control requires further technological development and therefore the publication of fully machine-based anonymised/pseudonymised decisions is, for now, restricted to internal use by the judiciary only.[59] In order to eliminate the risk of non-desirable results or negative consequences in terms of liability under data protection rules or reputational harm to data subjects, all published decisions in publicly available case-law databases still require human-administered control of the machine-produced results.

The format of judicial decisions and the extent of their standardisation or drafting procedure can have an impact on the level of automation involved in the anonymisation/pseudonymisation process. Judicial decisions often have a comparable structure: the elements comprise the parties and their respective roles, the date of the decision, the facts of the case, the legal considerations, the final decision, the names of the judge(s) and clerk, citations of cases and paragraphs of law, etc. Every lawyer is able to recognise these elements, although they are often not indicated explicitly. Unlike the lawyer, a computer is not capable of parsing a judgment that was drafted without a structured template into its constituent parts. Whether drafted by clerks, judges or computers, explicitly structured judgments offer several advantages:

- numbering of paragraphs facilitates referencing specific paragraphs of the judgment (both in writing and by use of a hyperlink that links to a specific, generally searchable or indexed, piece of web content on a website, rather than the website's home page (deep linking));

59. Only personnel within the judiciary; professional users such as advocates or citizens are not included.

- search results can be improved if searches can be performed on specific parts of the judgment;
- for a computer, understanding the syntax of a judgment is an indispensable first step in understanding the semantics and subsequently the legal reasoning of the judgment. This enables the development of sophisticated tools for legal reasoning, quality control and knowledge management.

Furthermore, greater use of a structured text can enable necessary links to the CMS, allowing for specific and indications of the personal data that should be replaced (or deleted) in the text. However, in order to achieve the desired results, the texts of the decisions will need to be adequately linked to the CMS and there must be the necessary interoperability between the systems.

Pseudonymisation of personal data of the parties (such as names or addresses) in the part of the decision containing the description of the parties involved and the facts of the case can be achieved rather easily using a machine-based solution. It is unlikely to interfere with the comprehensibility of the decision. However, the reasoning of the decision may prove to be more difficult, since inaccurate pseudonymisation or over- pseudonymisation by machine-based tools may affect the readability of the text and coherency/clarity of the argumentation. Pseudonymisation complications may occur particularly where personal data overlap with general terms, definitions or names. Additionally, the pseudonymisation of those indirect references which allow the drawing of conclusions about individuals pose significant challenges even for experienced judicial drafters and so will definitely be one of the biggest obstacles on the path to a fully machine-based procedure. Consider the following example, taken from an article discussing this issue:

> [I]n a criminal case concerning defamation and non-pecuniary damage the court cited a statement, which is considered as defamation "R. B. was a fictitious work supervisor who later copied her dissertations and other scholars' essays" („R. B. buvo fiktyvus darbo vadovas, kuris vėliau jos ir kitų mokslininkų disertacijas esą „nusirašė"). If we put this phrase [into] google search we immediately will find this phrase in the press and will be able to identify the parties in the case. This phrase was found in the most popular Lithuanian web page Delfi, and as you can see the parties are easily identified - R. Banevičius and Z. Migonienė.[60]

60. For more information and other examples: see Gruodytė E. and Milčiuvienė S. (2018).

Therefore, references to personal data in the reasoning of the decision should be avoided by using non-traceable paraphrasing by the (well-prepared) drafter, even if a future fully automated solution were to exist.

However, it will not be possible to fully avoid the possibility of re-identification through the context of the decision and the underlying case. Such re-identification may not always present a major privacy concern, though a number of risks may make it more egregious/harmful: data scraping, profiling of users and various forms of malicious use of information about data subjects, or discrimination against them based on the data collected from publicly open databases, etc.

Where such individual interference in private life does occur, it can be addressed through remedies available to the affected individuals, allowing them to have their particular case examined and their rights restored (see the description of the *Vicent Del Campo v. Spain* case above and Chapter IV below on risks related to publication and respective safeguards and remedies).

The following questions should be considered and addressed during the preparation of the anonymisation methodologies and tools.

1. Which set of personal data should be anonymised/pseudonymised (first name, last name, address, ID number, etc.)?
2. Which set of data besides personal data should be anonymised/pseudonymised (legal entity data, business secrets, state secrets, etc.)?
3. Should special categories of data be anonymised/pseudonymised and published?
4. Whose personal data should be anonymised/pseudonymised (defendant, witness, judge, lawyer, expert witness, third party, etc.)?

Chapter 4

Negative effects of publication and their mitigation

This report has highlighted the main concern faced in the publication of judicial decisions: fulfilling the goals and objectives of publication while guaranteeing data protection and privacy rights. This chapter will examine two key risks affecting these positions, alongside possible safeguards and remedies.

There are two important risks to consider in relation to the publication of judicial decisions, namely: i. technical and procedural failings resulting in personal data disclosure, and (ii) poor design of case-law data leading to difficulties searching and accessing judicial decisions.

1. Risks leading to disclosure of personal data and possible remedies

Having regard to the nature of the disputes brought before courts, the online availability of certain judicial decisions could put the right to privacy of individuals at risk and jeopardise the interests of the parties. Therefore, courts and judiciaries should ensure that appropriate measures are taken to safeguard data in conformity with the appropriate laws.[61]

61. CCJE (2011).

i. Risks

Pseudonymisation of judicial decisions does not represent a completely safe solution for personal data protection. A study carried out by researchers at the Massachusetts Institute of Technology, for example, revealed, in the context of work carried out on the bank card transactions of 1.1 million people with no identifying element, that four spatio-temporal data points (geographical co-ordinates, dates, times) alone made it possible to re-identify 90% of individuals.[62]

One possible method of re-identification is matching data from the database of published decisions with an archived schedule of court hearings, which often contains the names and other data of the parties. To address this risk, in some countries the database with the scheduled hearings does not contain information on the parties to the case, but only the case numbers. Online information boards showing published judicial decisions and public registers, such as those for property, may represent other sources of data risking re-identification.

In this regard, Recommendation Rec(2001)3 stipulates that access to information concerning court proceedings[63] should be accessible only to the parties to the case and other persons concerned. In terms of privacy, access should be restricted to the parties involved.

The online publication of judicial decisions carries the risk that personal data may be collected by third parties (namely scraped) from the publishing sources or websites. With high volumes of data being published regularly by courts of various instances, the need to consider and ensure the privacy protection of individuals involved or named in the proceedings is paramount. Even with safeguards in place, for example GDPR compliance, the publishing authority should consider the potential actions of third parties and private entities in relation to the data made public.

The risks of widespread data collection through data scraping can have a serious impact on the privacy rights of data subjects. There may be more direct consequences; for example, sensitive data such as genetic, financial and medical data, or data on gender, sexual orientation and ethnic origin may be used to harass or discriminate against a re-identified individual. Indirectly,

62. See *L'open data des décisions de justice*, p. 27, (French language only), available at www.science.org/doi/10.1126/science.1256297

63. The term "court proceedings" includes information on court procedures and internal rules, case information and communications with the courts.

sensitive data could enable profiling and so be used by third parties to analyse or predict aspects concerning the re-identified individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The eventual use of the data may not even be inherently malicious in intent – targeted advertising based on data collected without the user's consent is one such example.

The impact is not confined merely to the parties or data subjects themselves, it may affect the functioning of the judiciary itself. The harassment and intimidation of individual judges is a simple example. The use of data to profile individual judges goes further, attempting to draw correlations – real or supposed – between their personal characteristics, from gender to ethnicity to political opinions, and the reasoning for their decisions. Wide-scale dissemination of certain data could be used to attempt predictive analysis of a case outcome based on the judge hearing it, a practice that may often be mistaken and that may give rise to forum shopping.

There may even be a negative impact that arises indirectly from the non-malicious use of data. For example, court applications could be used to link and correlate the results of proceedings with the names of the parties' lawyers, allowing the determination of a ranking or success rate and in turn encouraging lawyers to select cases with the best chances of a favourable outcome, or to charge more for "risky" cases.

ii. Safeguards and remedies

The risks related to violations of personal data protection in the publication of judicial decisions require the provision of adequate safeguards and the availability of effective remedies, established in a suitable procedural framework.

Data protection – Guide to the case law of the European Court

Paragraph 212. The Court considers that the indiscriminate and open-ended collection of criminal record data is unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, *inter alia*, the duration of the storage of such data (ibid., paragraph 199).

A similar position is found in the jurisprudence of the CJEU.

> [L]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental rights to effective judicial protection.[64]

The procedural framework should introduce safeguards covering the range of personal data that may be handled and protected by judicial organisations, including: personal data made public in the publication of judicial decisions; the storage of the respective personal data in pseudonymised form in case-law databases; and the storage of full personal data in case management and other judicial systems.

Following on from this procedural framework, the "General principles concerning the protection of users of computerised legal information services" and the Guidelines for the relationship between a computerised legal information service and a user of such a service (in the appendix to the Committee of Ministers Recommendation No. R (83) 3 concerning the protection of users of computerised legal information services)[65] advise establishing a clear commitment and guarantee on behalf of the service provider. For instance:

- the relationship between the legal information service and the user should be regulated by rules provided in a contract, in standard contract clauses or in regulations. These rules should be made available in written form to a user at their request.
- every service should present to its users, on request, a document indicating the conditions which apply to the services it offers, which should include:
  - a guarantee that the service will not give to any person, unauthorised by the user, information regarding queries formulated by the user, subject to the legitimate use the service might make of the queries for its internal purposes;

As part of the procedural framework, special data protection authorities should be available to address the requests of data subjects to rectify or erase their data. As detailed in Chapters I and II, supervision of data processing operations can be entrusted to specific bodies within the judicial system, which should, in particular, ensure compliance with the applicable data protection rules.

64. Court of Justice case of 6 October 2015, *Maximillian Schrems v. Data Protection Commissioner,* C-362/14, ECLI:EU:C: 2015:650, paragraph 95.
65. Committee of Ministers (1983a).

The relevant body should also consider the implications for third parties of data protection violations as a result of publication and ensure their privacy rights are upheld.

Data protection – Guide to the case law of the European Court

Paragraph 251. In the case of *Vicent Del Campo v. Spain*, 2018 (paragraphs 53, 56), the fact that the applicant, a third party to judicial proceedings, had been deprived of any opportunity for asking a court, before delivery of the judgment, to refrain from communicating his identity had amounted to a violation of Article 8. The applicant had not been informed, questioned, summoned to appear or notified in any manner whatsoever.

The procedural framework for addressing such requests (providing remedies for persons wishing to have their personal data rectified or deleted) must also be effective.

Data protection – Guide to the case law of the European Court

Paragraph 297. The fact of imposing a requirement which creates an insurmountable barrier for a person requesting rectification of his identity data in the official State registers may be incompatible with the State's positive obligation to guarantee effective compliance with the right to respect for his private life (*Ciubotaru v. Moldova*, 2010, paragraphs 51-59).

The requests of data subjects should also be addressed by the competent authorities within a reasonable time.

Data protection – Guide to the case law of the European Court

Paragraph 303. The effectiveness of remedies available at the domestic level for persons wishing to have access to their personal data requires applications submitted by the data subjects to be processed within a reasonable time. In the case of *Roche v. the United Kingdom* [GC], 2005 (paragraphs 166-167, 169), the Court found a violation of Article 8 on account of an unreasonable waiting period for the applicant in accessing documents comprising personal data which would have enabled him to assess the potential risks to his health caused by his participation in military testing on gases.

Some practical options for possible safeguards in ICT systems and tools can be: allowing access to data only upon registration of the user; creating ways for identification of the user and tracing their actions with the data; and using replica databases on servers that are for public access.[66]

2. Risks linked to lack of adequate database structure, categorisation and classification of data

A high number of judicial decisions in the source database for publication could have a negative effect on the intended goals of publication, such as transparency, enhancement of legal certainty, strengthening of public scrutiny and access to precedents. This negative effect can occur if the underlying database is unusable or unsuitable for users due to deficiencies in its structure or in the processing of the legal texts. Examples of such deficiencies include the absence or poor classification and categorisation of texts in the database, incorrect or poor tagging of decisions and a lack of an effective search function. Therefore, thorough and well-designed automated tools and procedures for the classification and categorisation of judicial decisions, leading to a functional and accessible database, represent an important condition for open data and transparency.

The problem of an unsorted number of decisions in the database can be tackled from different angles.

i. Selection of decisions for publication

In order to minimise extraneous data in the database, a selective approach to publication can be taken to limit the decisions included to key judgments or important developments in the law. If a selective approach is considered some relevant requirements may be found in Recommendation No. R (95) 11 of the Committee of Ministers.

First of all, the selection of case law included in the databases (legal information retrieval systems) should be objective and representative: the selected decisions must be generally representative of the jurisprudence in the sector in question. This includes the selection of a decision that goes against a prevailing trend in jurisprudence.

66. Committee of Ministers (2001a).

Recommendation No. R (95) 11 proposes the following selection criteria.

- *Hierarchical selection*: the choice of decisions of one or several instances of courts according to their hierarchical status in the legal order of the country concerned.

A hierarchical selection for publication, which entails giving priority to decisions of higher courts, is a useful way of limiting the amount of information available for retrieval. However, it should be taken into consideration that the frequency of appeals may vary from one field of law to another and that certain types of cases cannot be appealed against. Therefore, decisions of lower courts should not be automatically excluded or overlooked.

- *Geographical selection*: the choice of decisions given by one or several courts selected according to their geographical location.

Geographical selection should be avoided unless particular circumstances justify the contrary, for example the existence of regional law or regional jurisdiction, or in the case of specific scientific research.

- *Selection by fields of law*: the choice of decisions in one or more fields of law, for example penal law, environmental law, procedural law, marriage law, fiscal law, etc.
- *Selection by substance*: the choice of court decisions according to whether they are or are not considered of sufficient legal interest.

Selection by substance should be applied only with great care so as to ensure the objectivity and representativity of the selection of the decisions. In this context "legal interest" means that a court decision expresses a rule of law. For example: setting a legal precedent, expressing a tendency of jurisprudence in the evaluation of facts, or (demonstrating) a procedural practice in such a way that the decision is or could be of importance for obtaining adequate and detailed knowledge of court practice in the field of law in question.

The following specific points should be taken into consideration when making selections:

- decisions entailing assessment (for example of the sentence, of damages), as well as decisions dealing mainly with questions of evidence or of contract should not be omitted, as a general rule, as these types of decisions represent some important elements of the legal systems.
- decisions expressing a "constant practice" of the courts should be represented in such a way as to reflect the main principles of the jurisprudence in the field concerned. On the other hand, this should not tend

to impede a possible evolution of case law. Consequently, the case-law databases should, at adequate intervals, store decisions that confirm or reverse a "firm practice" of the courts. Appropriate indications could be given, for example by adding annotations to texts confirming or changing the practice.

Recommendation No. R (95) 11 further provides that the selection should be carried out only according to established guidelines that are set up in advance, clearly defined and easily accessible to the users.

ii. Categorisation, classification and tagging

Proper categorisation and classification of texts in the database can significantly improve the experience of users, facilitating the searchability and analysis of the (selected) cases.

Recommendation No. R (95) 11 proposes the following elements on which to base the categorising and classifying cases, so as to enhance the functionality of the database:

- headlines;
- keywords;
- fixed vocabulary;
- abstracts;
- commentary: summary/analysis;
- notes (annotations), for example references to statute law, case law, doctrine;
- information on appeals and the result of appeals.

In general, a thorough approach to categorisation, classification and tagging of the published decisions can significantly contribute to the transparency of the judicial process. Unfortunately, the approach taken is often different in various courts and therefore the search function cannot be properly used. To overcome this, a centralised and agreed approach to categorisation, classification and tagging should be applied with regular revision of categories, classes, tags and keywords. Once the approach has been agreed, it should be communicated to all those who are involved in these processes and supported by easily accessible guidelines/manuals.

Chapter 5

Technological solutions – ICT development and implementation

The publication of judicial decisions and their pseudonymisation is almost impossible without making use of technological solutions. The development and integration of ICT into judicial processes is ongoing and information technology has become indispensable for the efficient functioning of the justice system. In its Opinion No. 14 of 2011 on justice and information technologies (IT),[67] the CCJE underlined that computerisation assists courts in rationalising file management as well as in registering and keeping track of cases. In this way, a series of files or connected cases can be managed under more secure conditions; templates may be designed to support the formulation of judicial decisions or orders; and multi-criteria statistics on each type of litigation can be gathered and made publicly available.

While this process can provide a lot of benefits and improvements to the judicial administrative process, some concerns need to be addressed.

1. **Privacy protection** – examined in Chapter II above.
2. **Human rights protection**, such as ensuring anti-discrimination practice and facilitating effective and efficient access to justice, is an important aspect that should be considered during the development of any kind of ICT.
3. **Judicial independence** is another important aspect that was underlined in Recommendation Rec(2001)2 of the Committee of Ministers to member states concerning the design and re-design of court systems and legal information systems in a cost-effective manner.[68]

67. CCJE (2011).
68. Committee of Ministers (2001a).

4. **User participation** and user friendliness of the results. The Committee of Ministers recommendation proposes including judges, Bar associations, notaries, court presidents and civil servants in the ICT development process.
5. **Project evaluation/assessment** during ICT development and integration to ensure it is fit for purpose and that it is properly implemented, maintained and updated.

From a practical implementation perspective, the following are specific questions that should be considered in the design and implementation of ICT systems within the legal data-processing context, as listed in Recommendation Rec(2001)2:

- how archiving will be organised;
- how to check the authenticity of documents and the identification of users;
- how far to modify procedures to suit the potential/limits of the new systems;
- how to arrange the migration/transfer of data between systems;
- how to ensure security of data and of the system, protection of personal data and to control access to data;
- how to link different systems (for example, CMSs and legal information systems);
- how to make use of the opportunities provided by internet, intranet, extranet, hyperlinks/XML.

1. Interoperability

The ICT tools for publication and anonymisation/pseudonymisation need to be interoperable (that is, able to exchange and make use of information) with other ICT systems used by the judiciary. Without adequate compatibility or interoperability, the very complex configuration of ICT architecture can necessitate the re-design of major parts or even all of the structure.

In this regard, the respective guidance in the Recommendation Rec(2003)14 of the Committee of Ministers to member states on the interoperability of information systems in the justice sector ("Recommendation Rec(2003)14") should be taken into consideration: such projects should be "implemented in the framework of co-ordinated programmes allowing for consistent actions to

be taken in various interconnected fields and among different stakeholders, thus ensuring the appropriate co-ordination and financing".[69]

The introduction of interoperability in the justice sector also requires appropriate changes to the relevant law and work process and adequate training of personnel.

Member states should provide for the establishment of audit or control points at relevant positions in the automated information and document flows inside and among the justice sector organisations. In the introduction of information technology, justice sector organisations should deploy the necessary human resources to make sound judgments on the proposed systems and services. Qualified personnel in charge of their information systems should ensure the respect of integrity, availability, storage and identification of electronic documents and data processed by the organisation concerned.

Special attention should be paid to data processing, which is vulnerable to increased risks in the context of interoperability with regard to information security and protection of privacy. Justice sector organisations should establish procedures to monitor and control potential exposure to risks arising from the misuse or failure of their information systems. These procedures should include security guidelines ensuring control of access to the various levels of their information systems.

The CMSs Of justice sector organisations should, in particular, be prepared for delivering information to and receiving it from other external CMSs, and for providing support in the decision-making process by enabling access to a complete range of relevant databases. Member states should facilitate the interoperability of various databases by introducing such unifying measures as unique identification codes and uniform data definitions.

2. Big data

Data contained in the databases of judicial decisions represent big data. Its processing and analysis can be a source of significant value and innovation. Since big data makes it possible to collect and analyse large amounts of data to identify attitude patterns and predict behaviours of groups and communities, the collective dimension of the risks related to the use of data should be considered.

69. Committee of Ministers (2003a), paragraph 3.3.

The Consultative Committee of Convention 108 drafted the Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data,[70] which provide a framework to apply appropriate policies and measures to make effective the personal data protection in the context of big data. Some of the recommendations from the guidelines pertinent to the publication of judicial decisions are provided below.

In the processing of personal data there is a need to balance all interests concerned, in particular where information is used for predictive purposes in decision-making processes. Controllers and processors should take into account the likely impact of the big data processing and its broader ethical and social implications to safeguard human rights and fundamental freedoms, and ensure the respect for compliance with data protection obligations.

In cases where there is a high impact of the use of big data on ethical values, controllers could establish an ad hoc ethics committee, or rely on existing ones, to identify the specific ethical values to be safeguarded in the use of data. The ethics committee should be an independent body composed by members selected for their competence, experience and professional qualities and for performing their duties impartially and objectively.

Authorities should take a precautionary approach in regulating data protection and adopting preventive policies concerning the risks of the use of big data and its impact on individuals and society. The preventive policies and risk assessment should consider the legal, social and ethical impact of the use of big data, including with regard to the right to equal treatment and to non-discrimination.

A risk assessment of the potential impact of data processing on fundamental rights and freedoms is necessary. This assessment process should be carried out by persons with adequate professional qualifications and knowledge to evaluate the different impacts, including the legal, social, ethical and technical dimensions. The assessment and the solutions proposed should be documented and made publicly available. When data controllers adopt open data policies, the risk assessment should take into account the effects of merging and mining different data belonging to different open data sets.

Controllers should regularly review the results of the assessment of the potential impact on fundamental rights and freedoms and the risk of re-identification, in the light of the technological development with regard to anonymisation techniques.

70. Consultative Committee of Convention 108 (2017).

The adoption of the solutions for the protection of the fundamental rights should be monitored.

The authorities should encourage the involvement of different stakeholders (such as individuals or groups potentially affected by the use of big data) in the assessment process and in the design of data processing.

3. Artificial intelligence

Currently, there is a growing tendency to apply machine learning algorithms and artificial intelligence in ICT, including in computerised judicial processes. These new technological developments also need to be scrutinised. In 2018, the European Commission for the Efficiency of Justice (CEPEJ) adopted its European ethical charter on the use of artificial intelligence (AI) in judicial systems and their environment.[71] The charter is intended for 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 (machine learning or any other methods deriving from data science). The charter lays out the five key principles that should be respected in the design and use of AI: 1. respect for fundamental rights in the design and use of AI tools; 2. non-discrimination; 3. data quality and security; 4. transparency, impartiality, and fairness; and 5. User control.

AI-based solutions may have consequences on individuals and society. Therefore, protection of human rights and fundamental freedoms, in particular the right to the protection of personal data, is essential during the development and adoption of such solutions. The focus should be on avoiding and mitigating the potential risks. Possible adverse consequences of AI applications on human rights and fundamental freedoms should be assessed by the stakeholders in charge of their development. A precautionary approach should be adopted, based on appropriate risk prevention and mitigation measures and considering these consequences.

The Guidelines on artificial intelligence and data protection[72] encourage developers, manufacturers and service providers to set up and consult independent committees of experts from a range of fields, as well as engage with independent academic institutions, which can contribute to designing human rights-based and ethically and socially oriented AI applications, and

71. CEPEJ (2018).
72. Consultative Committee of Convention 108 (2019).

to detecting potential bias. Also, risk assessment of such applications should be undertaken with the active engagement of the individuals and groups potentially affected by such applications.

The guidelines recommend that AI developers, manufacturers, and service providers:

adopt forms of algorithm vigilance that promote the accountability of all relevant stakeholders throughout the entire life cycle of these applications, to ensure compliance with data protection and human rights law and principles;

consult supervisory authorities when AI applications have the potential to significantly impact the human rights and fundamental freedoms of data subjects.

4. Training

As already mentioned above, continuous training of justice sector personnel in matters related to the application of information technology is an important element of ICT development in their organisations. In its Opinion No.(2011)14[73] the CCJE underlined that judges and court staff have both a right and a duty to initial and ongoing IT training so they can make full and appropriate use of IT systems.

Training is paramount for the successful integration of IT tools and their proper application. In this regard, Recommendation Rec(2001)3 sets out that the state should provide the necessary training and support services for the judiciary and staff involved in operating and using court and legal information systems.

Recommendation Rec(2001)2 proposes careful planning of user training needs from the very earliest phases of ICT projects. It also underlines the importance of effective training from the implementation phase onwards that should be planned in conjunction with user representatives.

Recommendation Rec(2003)14 provides that justice sector organisations should ensure that they inform their personnel of the relevant legislation and regulations which apply to the way information and data are handled within the justice sector. Incentives for personnel should be created to encourage them to use information technology applications in their daily work.

In the digital transformation process the training of justice professionals, including lawyers, has a vital role. It is important for both the efficiency and the

73. CCJE (2011).

independence of justice, because it allows justice professionals and lawyers to act with full knowledge of the law and procedures.

Equally important is the establishment of a help desk service. Also, the roles and responsibilities of the personnel of justice sector organisations regarding the use of information technology applications should be determined and clarified.

Chapter 6

Conclusions and checklist

Conclusion

Ensuring access to judgments through their publication, including online, plays a key role in safeguarding the right of access to justice (Article 6 of the Convention) as it increases the transparency of justice systems, secures public trust in them and contributes to consistency in case law. Publication should therefore be the default position. Privacy rights and data protection concerns remain a fundamental issue, yet can be addressed by the appropriate safeguards, remedies and tools; chief among these are anonymisation and pseudonymisation.

There is an abundance of different and complex issues that need to be considered when deciding whether anonymisation or pseudonymisation is needed and, if so, to what extent. At its core, the decision to be taken is one of a balancing act between meeting the goals of publication and securing data protection and privacy rights. At one extreme is the anonymisation of all personal data. However, the notion of personal data is too broad for this to be applied practically and may lead to the removal of large amounts of data in a way that would render decisions unreadable or meaningless. Overly broad anonymisation/pseudonymisation could contribute to the incomprehensibility of the reasoning of the court and limit the ability to consider the development of the law and future rulings, and hence would not contribute to the goals of publication.

At the other end of the spectrum is the simple publication of decisions as they are. Naturally, even in "non-sensitive" matters, namely where there is no formal requirement or rationale to exclude the public, there are issues that are personal to the parties involved and not of (significant) public interest which may be exposed or published. Additionally, broad data collection efforts alongside issues such as profiling present privacy concerns even with non-sensitive data.

Regardless of the decision taken on the balance to be struck, the design, development and implementation of the appropriate digital and ICT tools and processes also need to be considered. They must take account of and facilitate the various goals of publication, meet the end users' needs, and secure the various rights and interests of data subjects who are directly and indirectly affected.

The decisions to be made are a mix of the legal, practical and technological. It is up to the national authorities to consider the goals of publication and the balance with data and privacy protection, as well as to determine the appropriate methods and tools and their use and implementation. This report has examined a number of these decisions, contextualising the underlying positions and exploring the risks and solutions that will weigh in their determination. It is hoped this will provide guidance and direction to the decision makers as they engage in this essential and contemporary exercise.

Checklist

The checklist represents the list of questions that should be considered in the publication of judicial decisions and development of the respective ICT tools.

Regulatory framework

- ☐ Goals and objectives of publication are defined
- ☐ Regular assessments of the set goals and objectives are introduced to ensure that they have not lost their relevance and pertinence
- ☐ The scope of publication is defined (in all instances or only some; all decisions or only those which remain in force; all decisions or only specific ones selected by judges)
- ☐ Policies on publication are considered and formulated
- ☐ If publication is performed by a non-governmental entity, the respective arrangements are formulated and fixed concerning co-ordination with the judiciary and updates of the text in the database if and when needed
- ☐ A national legal framework regulating the protection of personal data is in place and coherent

Anonymisation/pseudonymisation

- ☐ Which methods of anonymisation/pseudonymisation are selected (for example, *ex ante* or *ex post*)

- ☐ The possibility to use a defined structure of judicial decisions to facilitate anonymisation/pseudonymisation is analysed and applied where possible (with respective training and incentives proposed for drafters of the texts of judicial decisions)
- ☐ The scope of pseudonymisation is defined (defendant, witness, judge, lawyer, expert witness, third party, etc.)
- ☐ The data that should be pseudonymised are defined (for individuals: first name, last name, address, ID number, special categories of data, etc.; for businesses: legal entity data, business secrets, state secrets, etc.)

Case-law database

- ☐ The frequency of updates with new decisions (preferably at least once per month) is defined
- ☐ In the case of selective publication of judicial decisions: the existence of set guidelines that are clearly defined and easily accessible to users
- ☐ A centralised and agreed approach is formulated to categorisation, classification and tagging of published decisions
- ☐ Guidelines describing how to categorise, classify and tag decisions before their publication are easily accessible and regularly updated
- ☐ Access to a complete range of relevant databases is enabled by introducing such unifying measures as unique identification codes and uniform data definitions
- ☐ Traceability of operations concerning the archiving of electronic documents is ensured
- ☐ Electronic document archiving systems are periodically assessed
- ☐ Entry, modification or deletion of electronic documents in electronic document archiving systems are undertaken by specialists authorised and trained to carry out such operations
- ☐ Uniformity is ensured in the document formats used (preferably open, international and standard, and permitting subsequent migration of data and allow processing in different languages)
- ☐ A retention period for personal data in the databases is defined
- ☐ The possibility is provided to address a request to rectify or delete data from the database
- ☐ Full anonymisation of judicial decisions after the set period is in place

ICT development and integration

- ☐ The necessary human resources for ICT development and maintenance are secured
- ☐ The roles and responsibilities of personnel in justice sector organisations regarding the use of information technology applications are determined
- ☐ Incentives are offered for personnel in justice sector organisations to encourage them to use the information technology applications in their daily work
- ☐ Project evaluation/assessment during ICT development and integration is arranged
- ☐ Human rights (including personal data) protection considerations are analysed, discussed and addressed
- ☐ Judicial independence considerations are analysed, discussed and addressed
- ☐ User involvement in the development process is ensured
- ☐ Audit or control points are established at relevant positions in the automated information and document flows
- ☐ Monitoring and control procedures are established in relation to potential exposure to risks arising from the misuse or failure of information systems (including security guidelines ensuring control of access to the various levels of an information system)
- ☐ Interoperability of CMSs is facilitated: they are prepared for delivering information to and receiving it from other systems and provide support in the judicial decision-making process by enabling access to a complete range of relevant databases
- ☐ An ad hoc ethics committee (an independent body) is established in cases where the use of big data has a high impact on ethical values, in order to identify the specific ethical values to be safeguarded in the use of data
- ☐ A risk assessment is undertaken of the potential impact of big data processing on fundamental rights and freedoms
- ☐ Preventive policies are adopted concerning the risks of the use of big data and its impact on individuals and society
- ☐ A help desk service is established
- ☐ In cases where AI elements are developed or integrated in the ICT tool(s), a risk assessment is implemented and consultations are held with supervisory authorities, individuals and groups potentially affected by the tool(s)

Security, safeguards and remedies

- ☐ Procedures are in place to ensure the physical protection of the premises where the electronic document archiving systems are situated, including adequate storage conditions and access control
- ☐ Special procedures are in place allowing the persons concerned to address a request to have personal data rectified or deleted
- ☐ Persons in charge of examination of requests to rectify or delete personal data in published judicial decisions are appointed and trained

Training

- ☐ User training needs are considered and planned from the very earliest phases of the ICT project, in conjunction with user representatives
- ☐ Continuous training and guides/manuals are proposed to the personnel involved in the publication of judicial decisions

References

Committee of Ministers of the Council of Europe

Committee of Ministers (1983a), Recommendation No. R (83) 3 of the Committee of Ministers to member States concerning the protection of users of computerised legal information services.

Committee of Ministers (1983b), Recommendation No. R (83) 10 of the Committee of Ministers to member States on the protection of personal data used for scientific research and statistics.

Committee of Ministers (1995), Recommendation No. R (95) 11 of the Committee of Ministers to member States concerning the selection, processing, presentation and archiving of court decisions in legal information retrieval systems.

Committee of Ministers (2001a), Recommendation Rec(2001)2 of the Committee of Ministers to member states concerning the design and re-design of court systems and legal information systems in a cost-effective manner.

Committee of Ministers (2001b), Recommendation Rec(2001)3 of the Committee of Ministers to member states on the delivery of court and other legal services to the citizen through the use of new technologies.

Committee of Ministers (2003a), Recommendation Rec(2003)14 of the Committee of Ministers to member states on the interoperability of information systems in the justice sector.

Committee of Ministers (2003b), Recommendation Rec(2003)15 of the Committee of Ministers to member states on archiving of electronic documents in the legal sector.

Other organs/bodies of the Council of Europe

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Consultative Committee of Convention 108) (2017), "Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data" – T-PD(2017)01, Directorate General of Human Rights and Rule of Law, 23 January 2017.

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Consultative Committee of Convention 108) (2019), "Artificial Intelligence and Data Protection: Challenges and Possible Remedies" – T-PD(2018)09Rev, Directorate General of Human Rights and Rule of Law, 25 January 2019.

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Consultative Committee of Convention 108) (2019), "Guidelines on Artificial Intelligence and Data Protection" –T- PD(2019)01, Directorate General of Human Rights and Rule of Law, 25 January 2019.

Consultative Council of European Judges (CCJE) (2004), Opinion No. 6 on fair trial and judge's role in trials taking into account alternative means of dispute settlement.

Consultative Council of European Judges (CCJE) (2011), Opinion No.(2011)14 on justice and information technologies (IT).

European Commission for the Efficiency of Justice (CEPEJ) (2018), "European ethical charter on the use of artificial intelligence in judicial systems and their environment" – CEPEJ(2018)14.

European Union

European Agency for Fundamental Rights (EU FRA) (2018), Handbook on European data protection law.

European Union (2012), Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

European Union (2016a), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

European Union (2016b), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

European Union (2019), Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

European Union (2023), The 2023 EU Justice Scoreboard, European Commission, June 2023.

Gruodytė E. and Milčiuvienė S. (2018), "Anonymization of court decisions in the EU: actual and comparative issues", *Law Review*, January 2018.

Further reading

Committee of Ministers (2018), Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.

Committee of Ministers (2019), Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes – Decl(13/02/2019)1.

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

Committee of Ministers (2021), Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

European Commission against Racism and Intolerance (ECRI) (2018), "Discrimination, artificial intelligence, and algorithmic decision-making", Directorate General of Democracy, November 2018.

Parliamentary Assembly (2017), Recommendation 2102 (2017) of the Parliamentary Assembly on technological convergence, artificial intelligence and human rights.

Parliamentary Assembly (2020a), "The brain-computer interface: new rights or new threats to fundamental freedoms?", Committee on Legal Affairs and Human Rights, 24 September 2020.

Parliamentary Assembly (2020b), "Preventing discrimination caused by the use of artificial intelligence", Committee on Equality and Non-discrimination, 29 September 2020.

Parliamentary Assembly (2020c), "Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems", Committee on Legal Affairs and Human Rights, 1 October 2020.

Steering Committee on Media and Information Society (CDMSI) (2019), "A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework" – DGI(2019)05.

Ensuring access to judgments through their publication, including online, plays an important role in safeguarding the right of access to justice (Article 6 of the European Convention on Human Rights). It increases the transparency of justice systems, secures public trust in them and contributes to consistency in case law. Privacy rights and data protection concerns remain a fundamental issue, yet can be addressed by the appropriate safeguards, including anonymisation and pseudonymisation.

A balance must be struck between meeting the goals of publication and securing data protection and privacy rights. In so doing, the design, development and implementation of the appropriate digital tools and processes should also be considered. They must take account of and facilitate the various goals of publication, meet the end users' needs and secure the various rights and interests of data subjects who are directly and indirectly affected.

This publication presents a compilation of existing standards and recommendations, including those of the Council of Europe, concerning the online publication of judicial decisions, personal data protection in published decisions, anonymisation and pseudonymisation, risks related to publication and their mitigation, and technological tools development.

Iceland Liechtenstein Norway grants
Norway grants

PREMS 098823

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE