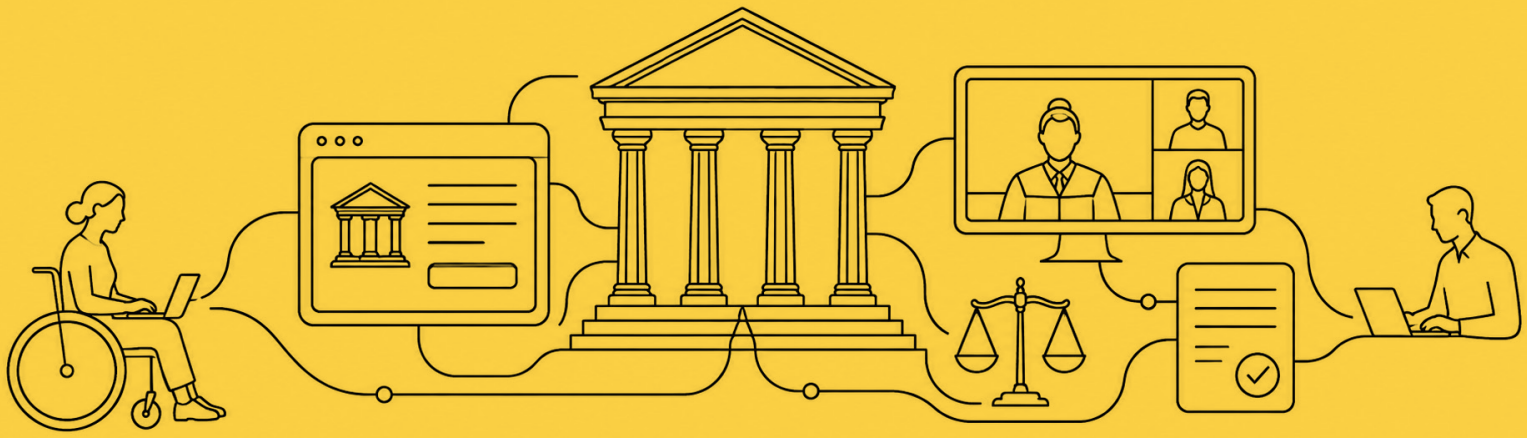
ELI
EUROPEAN
LAW
INSTITUTE

Principles on the Digitalisation of Civil Justice Systems in Europe

European Law Institute



The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment, it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

President: Teresa Rodríguez de las Heras Ballell
First Vice-President: Sir Geoffrey Vos
Second Vice-President: Pietro Sirena
Treasurer: Anne Birgitte Gammeljord
Speaker of the Senate: Reinhard Zimmermann
Secretary-General: Vanessa Wilcox

Scientific Director: Christiane Wendehorst

European Law Institute
Schottenring 16/ 175
1010 Vienna
Austria

Tel: + 43 1 4277 22101
E-mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

Approved by the ELI Council on 20 July 2026 and by the ELI Membership on 7 September 2026.

Published on 6 October 2026

ISBN: 978-3-9505990-6-0
© European Law Institute 2026

This publication was co-funded by the European Union's Justice Programme. Acknowledgement is also due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011. Views and opinions expressed are those of ELI 's only and do not necessarily reflect those of the European Union, the University of Vienna or others. Neither the European Union nor others can be held responsible for them.

universität wien

This project is co-funded by the European Union

Table of Contents

Acknowledgements **5**

Preface **7**

Executive Summary **8**

Part I – Fundamental Principles **9**

Principle 1: Aim and Scope 9
Principle 2: Fundamental Rights and Values Enhancement 9
Principle 3: Equal Access to Digital Justice 10
Principle 4: Judicial Impartiality and Independence 11
Principle 5: Fair Civil Justice 12
Principle 6: Public Justice 13
Principle 7: Justice within a Reasonable Time and at Reasonable Expense 14

Part II – Design Principles **16**

Principle 8: Effective Governance 16
Principle 9: Digital Design 17
Principle 10: User-Centric, Inclusive and Data-Driven Design 19
Principle 11: Public and Private Integration 20
Principle 12: Data Standards and Interoperability 21
Principle 13: Enhanced Accessibility 22
Principle 14: Enhanced Transparency and Accountability 25
Principle 15: Artificial Intelligence 27

Part III – Implementation and Operational Principles **29**

Principle 16: Iterative Evolution and Piloting 29
Principle 17: Evaluation 30
Principle 18: Effective Training and Guidance 31
Principle 19: Sustainable Funding 32
Principle 20: Digital Sovereignty, Data Protection and Security 33

Acknowledgements

Project Team

Reporters
Masood Ahmed (Reporter; Professor, The United Kingdom)
Xandra Kramer (Reporter; Professor, The Netherlands)
Jiří Novák (Reporter; Lawyer, Czech Republic)
Dory Reiling (Lead Reporter; Judge, The Netherlands)
John Sorabji (Reporter, from January 2025; Professor, The United Kingdom)

Assistants to the Project Team
Peter Homoki (Lawyer, Hungary)
Anna Skrjabina (Consultant, Latvia) (Project Reporter from January 2024 to February 2025)
Marco Velicogna (Researcher, Italy)
Iain G Mitchell KC (Lawyer, The United Kingdom)
Blerina Bulica (Civil Servant, Albania)
Ioana Cornescu (Lawyer, Romania)
Emma van Gelder (Professor, The Netherlands)

Advisory Committee

Assessors
Lorena Bachmaier-Winter (Professor, Spain)
Teresa Bielska-Sobkowicz (Judge, Poland)
Matthias Neumayr (Professor, Austria)
Sir Geoffrey Vos (Judge, The United Kingdom)

Other Members of the Advisory Committee
Giulio Borsari (Civil Servant, Italy)
Natalie Byrom (Researcher, The United Kingdom)
Brett Dixon (Lawyer, The United Kingdom)
Martin Ebers (Professor, Germany)
Simone Ginzburg (Consultant, Bosnia and Herzegovina)
Iliana Kosti (Lawyer, Greece)
Jean Lassègue (Researcher, France)
Victoria McCloud (Lawyer, The United Kingdom)
Anna Nylund (Professor, Norway)
Giesela Rühl (Professor, Germany)
Rimantas Simaitis (Professor, Lithuania)
John Sorabji (Professor, The United Kingdom; until January 2025)
Eva Storskrubb (Professor, Sweden)
Jelle van Veenen (Innovation Manager, The Netherlands)
Jin Ho Verdonschot (Researcher, The Netherlands)

Members Consultative Committee
Peter Adler (Mediator, Austria)
Arvind Babajee (Accountant, Mauritius)
Lorena Bachmaier-Winter (Professor, Spain; MCC Chair)
Ole Böger (Judge, Germany)
CORPME (represented by Marta Hernández)
Boyan Dachev (Insurance Professional, Bulgaria)
Anna van Duin (Professor, The Netherlands)
Alessandra De Luca (Professor, Italy)
Marco Giacalone (Professor, Belgium)
JusGov (Research Centre, Portugal)
Rónán Kennedy (Professor, Ireland)
Nicolas Kyriakides (Professor, Cyprus)
Sebastian Schwamberger (Professor, Austria)
Nathalie Smuha (Professor, Belgium)
Inesa Stolper (Researcher, Lithuania)
Sophie Turenne (Professor, The United Kingdom)
Wannes Vandenbussche (Professor, Belgium)
Sjef van Erp (Professor, The Netherlands)
Jim van Mourik (Professor, The Netherlands)
Irina Zlatescu (Professor, Romania)

Observers

European Commission (represented by Katerina Entcheva)
European Commission for the Efficiency of Justice (CEPEJ, represented by Daniel Schmidt)
European Network of Councils for the Judiciary (ENCJ, represented by Claudiu Dragusin)
Justice Administration Research Association (represented by Alina Ontanu)
The International Institute for the Unification of Private Law (UNIDROIT, represented by Anna Veneziano)

ELI Project Officer
Tomasz Dudek (Senior Project Officer, Austria)

Preface

These European Law Institute (ELI) Principles concern the Digitalisation of Civil Justice in Europe. They take as their point of departure the fundamental rights laid down in Article 6(1) of the European Convention on Human Rights (ECHR) and Article 47 of the EU Charter on Fundamental Rights (EU Charter), and build on the ELI-UNIDROIT Model European Rules of Civil Procedure and on existing studies of digitalisation of justice systems. In an increasingly digitalised society, the need for digitalisation of justice is self-evident. In recent decades, governments across Europe have invested in digitalising justice. Within the European Union there has, equally, been a considerable focus on the digitalisation of justice. Nevertheless, civil justice systems across Europe remain in different states of development and therefore have different needs. Moreover, there is significant room for improvement. Matching technology to legal needs, including the protection of fundamental rights, and ensuring that digitalisation is not primarily viewed as a means to save costs and increase efficiency but rather that it is a means to promote such objectives to better secure access to justice, is complex. These Principles are intended to provide an overarching framework to guide the ongoing digitalisation of European civil justice systems. They are particularly intended to support digitalisation in European countries, European Union member states, as well as other countries, to increase interoperability between justice systems, and to safeguard fair justice delivery and fair procedures.

Executive Summary

The European Law Institute *Principles on the Digitalisation of Civil Justice Systems in Europe* provide a coherent, rightsbased framework to guide the design, implementation and operation of digital civil justice systems at national and European levels. They respond to the uneven pace of development and form of digitalisation within Europe, and the need to ensure that technological innovation strengthens and expands access to justice, the rule of law and fundamental rights and values.

The Principles take as their foundation Article 6(1) of the European Convention on Human Rights, Article 47 of the EU Charter of Fundamental Rights, and the ELIUNIDROIT Model European Rules of Civil Procedure. Digitalisation is understood not merely as a tool for efficiency or cost reduction, but as a means to enhance equal and effective access to justice, judicial independence, procedural fairness and public confidence in the delivery of civil justice. The Principles apply to civil justice systems specifically, but may be equally applicable to administrative justice systems, and include all stages of dispute prevention, court proceedings and enforcement. While they are primarily directed at public justice systems, they recognise the importance of integrating noncourt dispute resolution both at the pre-court stage of disputes and during court proceedings.

The Principles are divided into three Parts. **Part I** identifies Fundamental Principles. They establish that digitalisation must enhance fundamental rights and values. Thus, they identify the need for digitalisation to: secure equal access to justice, including for vulnerable and digitally excluded users; safeguard judicial impartiality and independence; promote fair and public justice; and, improve the civil justice system's ability to secure effective dispute resolution and (where necessary) enforcement within a reasonable time and at reasonable cost. They also require that digital civil justice must remain inclusive, with nondigital alternatives and practical support available where required.

Part II sets out the Principles that should govern the design of digitalisation. They emphasise effective governance and a digital by design approach to digitalisation, which should be informed by inclusivity and usercentricity. They stress that its design should be evidencebased. These Principles also stress the importance of interoperability, technologyneutral data standards, and the integration of public and private dispute resolution mechanisms. Digital justice systems should furthermore be designed to enhance accessibility through multilingual access, secure digital communications, online hearings, digital enforcement and free public access to judgments. Transparency and accountability are to be promoted through, for instance, digital court listings, access to case information, live streaming and recording of hearings, and the publication of machinereadable judgments. Particular care is taken within the Principles to emphasise the positive benefits of the appropriate and ethical use of Artificial Intelligence (AI), which should assist and augment the delivery of justice, but not replace judicial decisionmaking absent fully informed party consent.

Finally, **Part III** identifies Principles to govern the implementation and operation of digitalised civil justice. They emphasise that digitalisation is a continuous process, which requires iterative development, piloting, evaluation and sustained investment in people, infrastructure, training and guidance if it is to be fully effective. They also make clear that digitalisation should enable the effective evaluation of the delivery of digital justice if it is to give effect to the fundamental principles contained in Part One. Sustainable investment and funding are identified as necessary features of effective digitalisation. Finally, the Principles stress the critical importance of digital sovereignty, data protection and security, including robust governance structures, differential access controls and independent oversight mechanisms.

The *Principles on the Digitalisation of Civil Justice Systems in Europe* provide a principled and practical roadmap for the digital transformation of European civil justice systems. Their application will ensure that technological change serves justice and the rule of law.

Part I – Fundamental Principles

Principle 1: Aim and Scope

1. *These Principles are intended to guide and improve digitalisation of European civil, including commercial, justice systems. They may also apply to administrative justice systems. They encompass all stages of effective dispute resolution before, during and after the conclusion of court proceedings, which includes enforcement.*

2. *The digitalisation of civil justice systems (digitalisation) includes designing, developing, and implementing information technology in those justice systems.*

Comment

1. The digitalisation of civil justice systems has developed at different speeds throughout Europe and has different modalities. Where EU legislation is concerned, it focuses primarily on judicial cooperation in the cross-border context,[1] while there is no consistent approach in European soft law instruments.[2]

2. This Principle lays down the aim and scope of these Principles, which serve as a guide for regulating consistent and effective digitalisation of civil justice systems, including the use of AI, both at the European and national level. The Principles cover all stages of domestic and cross-border civil, including commercial, proceedings. They apply to: the provision of relevant legal information before initiating proceedings and the enforcement of court decisions. While it is acknowledged that different types of disputes may require a different approach, for instance those in the areas of administrative or insolvency law,[3] these Principles may also serve as guidelines for such disputes. They have not been designed for use in criminal law.

3. By information technology the Principle is intended to refer to, for instance, the use of electronic, telecommunications and computer technology.

Principle 2: Fundamental Rights and Values Enhancement

1. *Digitalisation should serve the purpose of enhancing the capacity of European civil justice systems to safeguard public and private law rights, including fundamental rights and values. In particular, it should promote the effective and consistent protection of the rule of law in line with fundamental procedural principles.*

2. *Safeguarding fundamental rights and values and the rule of law includes:*

   a. *the resolution of a dispute through a court decision and, where necessary, the enforcement of that decision;*

[1] See EU Regulation 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial, and criminal matters, and amending certain acts in the field of judicial cooperation.

[2] See CEPEJ, *Guidelines on electronic court filing (e-filing) and digitalisation of courts*, (2021); CEPEJ, *Guidelines on videoconferencing in judicial proceedings*, (2021); CCJE, *Moving Forward: The Use of Assistive Technology in the Judiciary*, (Opinion No 26, 2023).

[3] On the requirements for digitisation in insolvency, see Directive (EU) 2019/1023 EU (Directive on restructuring and insolvency) esp, Article 28.

b. the resolution of legal disputes, whether before or during legal proceedings (including any enforcement proceedings) by party agreement; and

c. the prevention of disputes by making court judgments available to the public.

Comment

1. Digitalisation offers opportunities to make access to justice more effective and efficient and strengthen the rule of law. The design and use of information technology should thus support fundamental values of civil justice, in particular the right to a fair trial as laid down in Article 6(1) of the ECHR and Article 47 of the EU Charter as well as that of EU instruments on civil procedure.[4] Paragraph 2 non-exhaustively sets out elements that are essential in the context of digitalisation of justice.

2. Paragraph 2(a) refers to the right of access to a court, including enforcement. While these Principles primarily involve dispute resolution through courts, paras. 2(b) and (c) recognise the contribution a digitalised system can make beyond court proceedings. Paragraph 2(b) thus refers to the promotion of the public interest in the consensual settlement of disputes, which is itself a fundamental value. It can be promoted through increasing access to the civil courts and to the public availability of judgments, as well as the incorporation of consensual forms of dispute resolution into the civil court process, through digitalisation. Paragraph 2(c) refers to the public interest in the proper prevention of disputes by enabling citizens to order their affairs by promoting increased understanding of legal rights and obligations.

Principle 3: Equal Access to Digital Justice

1. Digitalisation should enhance the civil justice system's ability to secure a person's right of equal access to justice. States must facilitate access to justice by appropriate digital means.

2. Digitalisation should safeguard the rights of vulnerable people. This should be achieved through the provision of technical and practical assistance, including non-digital means by which equal access to justice can be secured where necessary.

Comment

1. The right to digital access to justice, as such, has not (yet) been recognised in the case law of the ECHR or the EU Charter, but it is widely acknowledged that the use of digital tools can foster the right of effective access to justice.[5] For instance, the European Court of Human Rights (ECtHR) has acknowledged that digital technology may be helpful in supporting the administration of justice and promoting the fundamental rights laid down in Article 6 ECHR.[6] Additionally, the EU has stated that: '*Effective access to justice is a core objective of the area of freedom, security and justice. Digital transformation is a key step towards improving access to justice and the efficiency, quality and transparency of justice systems*'.[7] This Principle goes beyond such statements. It emphasises that digitalisation is more than helpful and more than a means to promote efficiency or other instrumental aims, but rather that it is a means

[4] Eg Article 1(1) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast); Regulation (EU) 2020/1784 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (recast); Regulation (EU) 2020/1783 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence) (recast).

[5] See, among others, *Airey v Ireland* (1979) 2 EHRR 305.

[6] *Xavier Lucas v France*, no 15567/20 (ECtHR).

[7] Regulation (EU) 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, Recital 7.

to promote equal and effective access to justice. It emphasises that access to digital justice is a right. In these Principles, this right of access should be understood broadly, consistent with Principle 2, para. 2.

2. Paragraph 1 obliges states to support the fundamental right of access to the civil justice system by appropriate digital means, eg reliable web portals, chat platforms, chatbots, electronic case management systems, and video conferencing (see Principle 13). Such tools should, particularly, be designed to support the bringing of a case to court in the swiftest, simplest, and most cost-effective way possible. This requires careful design (Principle 10).

3. Paragraph 2 focuses on the importance of ensuring that digitalisation is inclusive and is neither designed nor implemented in ways that are detrimental to vulnerable individuals or groups, including less digitally literate citizens, those who have no, or less advanced, technical equipment, or who have impairments that may make access to, or the use of, digital sources and equipment difficult. To that end, digital justice design should, through a commitment to user-centric design,[8] take into account the needs of vulnerable people, securing for them transparency, non-discrimination, privacy, and accountability. Further to this, practical and technical support should be made available. This should include: (a) access to the justice system in non-digital form where necessary; and (b) support for people who have (i) limited technical skills, (ii) limited or no access to appropriate technical equipment, or (iii) are less literate or have cognitive, visual or auditory needs (Principle 13).

Principle 4: Judicial Impartiality and Independence

1. *Digitalisation should enhance judicial impartiality and independence. To realise this, the judiciary should have a decisive role in any digitalisation design process. They should, particularly, be responsible for determining the objectives, applications and implementation of digital technology within the civil justice system.*

2. *Digitalisation should also improve judicial transparency and accountability.*

3. *Responsibility for giving effect to paragraph one should be entrusted to specific judges who have appropriate technological and managerial experience.*

Comment

1. Digitalisation can, and should, support judicial impartiality and independence with procedural transparency and accountability. Independence and accountability go together: accountability is a prerequisite for independence.[9]

2. Technology supports accountability in various ways, eg through online streaming of hearings that raise public interest issues and the online publication of judgments, of judges' outside interests, of court statistics, and information concerning the nature, structure and organisation of the courts and judiciary (Principles 5, 6 and 20).[10] Impartiality can, particularly, be promoted through enabling parties to obtain access to case materials and

[8] See also OECD, *Framework and Good Practice Principles for People-Centred Justice*, (2021).

[9] European Network of Councils for the Judiciary (ENCJ), *Indicators Independence, Accountability and Quality of the Judiciary*, (2023).

[10] N Byrom, *Report on the Impact of COVID-19 on Civil Court Users*, (Civil Justice Council, 2020); A Wallace & K Laster, *Courts in Victoria, Australia, During COVID: Will Digital Innovation Stick?*, (2021) 12 International Journal for Court Administration 9; Meeting of Chief Justices Judicial Group on Strengthening Judicial Integrity, *Bangalore Principles of Judicial Conduct*, (2002). United Nations Office on Drugs and Crime UNODC, *Commentary on the Bangalore Principles of Judicial Conduct*, (2007); P. Langbroek & M. Fabri, *Is There a Right Judge for Each Case?*, https://cadmus.eui.eu/bitstream/handle/1814/7713/EJLS_2007_1_2_12_FAB_EN.pdf?sequence=1; CCJE (2023).

documents that have been filed digitally, ie through access to digital case files.[11] Such materials can also contribute to accountability and transparency through the collection and analysis of case-related information that concern key performance indicators, such as those relating to case disposition times (see Principle 7).

3. To ensure that digitalisation, particularly where the design of digitalised systems is concerned, does not undermine judicial impartiality or independence, it is essential that designated judges, who have relevant experience, have a decisive role in any decision-making process concerning digitalisation programmes (Principle 18).

Principle 5: Fair Civil Justice

1. *Digitalisation should enhance the fairness of civil justice systems, including the right to a fair court procedure, hearing and judgment. It should increase:*

   a. *the effective participation of all those involved in the process of resolving civil disputes. This should be done through the use of digital forms of assistance and guidance; and*

   b. *the efficient and cost-effective transfer of party and dispute-related information, including that relating to enforcement, from non-court-based dispute resolution processes to the digital civil justice system.*

2. *To preserve legal professional privilege and any other relevant protected interests, including data protection rights, access to any information transferred to or held by the digital civil justice system should be capable of being restricted as necessary to preserve those privileges or rights.*

Comment

1. Digitalisation of civil justice systems should be geared to support access to, and the quality of, dispute resolution. This Principle therefore requires the design and implementation of digital technology to actively promote the right to a fair court procedure consistently with Article 6 ECHR, Article 47 EU Charter and national law.

2. Paragraph 1(a) therefore requires digitalisation to guarantee parties and their representatives digital access to documents relating to the dispute and other information relevant for the procedure. This can be achieved, for instance, through an accessible and secure court web portal (Principle 13). Provision is also required for hearings to take place in-person in a court room, via video conferencing or a digital platform, audio conferencing, or a combination of these methods. Where parties are not represented by lawyers, online platform design, including the provision of, for instance, chatbots, should provide assistance and guidance so that those unrepresented parties can secure effective access and equality of arms.[12]

3. Paragraph 1(b) emphasises that a fair civil process is one that facilitates the smooth and timely transfer of party and dispute-related information, within the boundaries of confidentiality, from non-court-based dispute resolution procedures to the digital court system (Principle 11). This applies regardless of whether the non-court-based dispute resolution procedure is a consensual or mandatory process carried out prior to court proceedings.

[11] AD (Dory) Reiling, *Court Information Technology: Hypes, Hopes and Dreams* in *New Pathways to Civil Justice in Europe*, (2021) 43.

[12] See ECtHR *Kerojärvi v Finland*, no. 17506/90 and *Fretté v France*, no. 36515/97, requiring special attention to effectively secure the rights of parties not represented by lawyers. Examples of (semi) public or private initiatives are *Demander justice* in France (https://www.demanderjustice.com/), *Rechtwijzer* in the Netherlands (https://rechtwijzer.nl/) and *Wikivorce* in the United Kingdom (https://divorce.wikivorce.com/advice).

4. To secure a fair process, it is also essential that digital communication systems protect confidentiality and professional privilege.[13] Technology used must therefore be designed in a way that reinforces trust in such confidentiality as is essential to upholding the rule of law. For example, in the case of online hearings, to maintain confidentiality, break-out rooms may provide space for a client to obtain advice from their lawyer. A precondition of such break-out rooms is that they are neither recorded nor available to anyone outside of the break-out room, and that this is clearly communicated to maintain trust.

Principle 6: Public Justice

1. *Digitalisation can enhance the right to public justice. It should improve:*

   a. *the open and public nature of interim and final hearings;*

   b. *the public accessibility of court documents, judgments, and orders; and*

   c. *the identification of outcomes of legal proceedings, particularly to facilitate the identification and publication of information that can help promote dispute prevention, the early resolution of disputes through non-court-based dispute resolution, and, where necessary, judgment.*

2. *The right to public justice can be limited to protect valid interests, as defined by law. Digitalisation should therefore make provision for appropriate and effective technological safeguards that facilitate necessary lawful restrictions, either fully or partially, of access to hearings, court documents, decisions, judgments and orders to protect those interests.*

Comment

1. The right to public justice is inherent in the right to a fair trial. It is well established in all European legal traditions.[14] While implemented differently throughout Europe, it generally: requires hearings to be held in public; ensures public and media access to, and reporting of, proceedings; and provides access to judgments, other court decisions and court documents.

2. Several important rationales underpin the right to public justice. It promotes democratic accountability of, and public confidence in, the civil courts and judiciary.[15] It protects parties against the administration of justice in secret.[16] Thus, rendering the administration of justice visible, a public hearing contributes to achieving a fair trial.[17] It may also help promote fair civil justice through reducing the likelihood of parties or witnesses making unfounded claims or inaccurate or untruthful statements during civil proceedings, while additionally helping to bring proceedings to the attention of potential witnesses and parties who might otherwise be unaware of them.[18] The right to public justice further promotes public understanding of the law and its application, helping to provide the secure framework through which citizens order their affairs on a sound legal basis, while also promoting democratic debate through helping to bring court decisions to public attention. By forming a part of public legal literacy,

[13] CCBE Code of Conduct, in particular Article 2.3.1.

[14] See Article 6 ECHR; Article 47 EU Charter; *Scott v Scott* [1913] AC 417 (the United Kingdom); Article 24, para 2 Spanish Constitution; Article 20(1) Constitution of Greece; and Article 96(2) Constitution of the Czech Republic. And see Article 11 Universal Declaration of Human Rights; Article 14 International Covenant on Civil and Political Rights; ALI/UNIDROIT Principles of Transnational Civil Procedure (CUP, 2006), Principle 20; ELI/UNIDROIT Model European Rules of Civil Procedure (OUP, 2021), r 17.

[15] CCJE, *On the position of the judiciary and its relation with the other powers of state in a modern democracy*, (Opinion No 18 of 2015) at [27]-[28] and [32].

[16] *Straume v Latvia* App no 59402/14 (ECtHR, 2 June 2022) at [124].

[17] *Malhous v Czech Republic (GC)* App no 33071/96 (ECtHR, 12 July 2001) at [55]–[56].

[18] J Jaconelli, *Open Justice*, (2002, OUP).

it also helps promote the formation of disputes, where that is appropriate, as it increases the likelihood that citizens are aware of their rights and obligations and how to resolve disputes through consensual means or via litigation.

3. Digitalisation of the civil justice system should be carried out to improve the implementation of the right to public justice. Care, however, needs to be taken to minimise the risk of harm to fundamental rights and values that digitalisation could create. Greater transparency through digitalisation could, for instance, provide a means through which individual judges could be profiled with judgment analytics being used to predict their behaviour in court and, hence, shape litigation strategies. It could enable parties and witnesses to be targeted, thus improperly interfering with the administration of justice. It could also result in increased and lasting public knowledge of individuals' private and family life when they are involved in civil proceedings. To that end, paragraph 2, stresses the importance of digitalisation being implemented in such a way as facilitates necessary and lawful restrictions on public access to digitalised proceedings. Such restrictions may include anonymisation in appropriate cases, consistent with the need to protect valid public and private interests, as defined by law. It should thus be consistent with Principles 2 and 4. Principle 14 sets out how public justice can be promoted within the framework provided by this Principle.

Principle 7: Justice within a Reasonable Time and at Reasonable Expense

Digitalisation should improve the delivery of effective dispute resolution within a reasonable time and at reasonable expense by improving, amongst other things, the civil justice system's ability to digitally:

a. manage individual proceedings, identify and manage collective proceedings, and the court's overall caseload. Individual judges should have access to information to help them identify how they can manage proceedings effectively;

b. identify and set standards and targets for the timely resolution of proceedings at reasonable expense for the parties and provide the means to promote effective compliance with their achievement by the court and parties to proceedings;

c. identify appropriate court and non-court-based methods to resolve disputes and, where appropriate, facilitate their implementation;

d. identify where, and in what circumstances, proceedings are not progressing in a timely or cost-effective manner; and

e. collect, analyse, and provide statistical information concerning the length of all stages of proceedings both at an individual and systems level.

Comment

1. Judgment within a reasonable time is first and foremost a human right. Timely disposition of disputes also has value to the economy. Long disposition times are one of the main complaints regarding court performance.

2. Digitalisation should be utilised to provide the means by which parties and the judiciary can improve efficiency and reduce disposition time. This is particularly the case where digital case management systems can help facilitate the provision and sharing of information between

parties and the court, which evidence shows reduces case disposition times.[19] They can also facilitate case weighting and categorisation systems by providing information on disposition times, processing and waiting times, clearance rates, and backlogs and thus promote effective management of disputes and more efficient judicial and court administration.[20] They can, particularly, help identify and reduce delay by identifying procedural bottlenecks and facilitating the evaluation of judicial interventions.[21] Time standards for case types, measuring, keeping track of adherence to those standards, and access to information about case management are also all proven ways of using technology to improve disposition times. Such measures should be adopted further to this Principle.

3. To further give effect to this Principle, statistical data and indicators should be presented in the form of digital dashboards. These are valuable monitoring tools that provide consolidated statistical data on court performance. They can be set up at the national, court, or judge levels.

[19] AD (Dory) Reiling (2009); implementation of such systems should be consistent with the approach and order set out in ELI/UNIDROIT (2021), r 47 to 49.

[20] CEPEJ, *European Judicial Systems - CEPEJ Evaluation Report - 2024 Part 1: General Analyses* (2024); A Cordella & F Contini, *Digital Technologies for Better Justice*, (Interamerican Development Bank, 2020) Discussion Paper No IDB-DP-761 <https://doi.org/10.18235/0002297>.

[21] The provision of such information is part of the judiciary's duty of accountability (Principle 4).

Part II – Design Principles

Principle 8: Effective Governance

1. *Digitalisation requires effective governance throughout its lifespan to safeguard Principles 2 to 7. This includes effective governance of the digital civil justice system's design, design team, implementation (including those responsible for carrying it out), operation, and ongoing evaluation and improvements to it once operative.*

2. *Effective governance requires a commitment to, and implementation of, good practice in project management and digital transformation by the state body responsible for digitalisation and, where that is not the judiciary, the judiciary.*

3. *Effective governance requires risk assessments to identify the benefits and risks of digitalisation, including risks to judicial independence and equal access to justice. Proportionate steps should be taken to minimise and/or mitigate risks and, conversely, to secure the benefits of digitalisation.*

4. *Once digitalisation is effected, the judiciary and the court administration should utilise judicial and court performance data to promote fair and timely justice service delivery by effective resource planning, case management, hearing scheduling and to protect judicial independence.*

Comment

1. Effective management of any major project, of which digitalisation projects are paradigm cases, is essential if they are to have any real prospect of success. To best promote success, it is essential that digitalisation is overseen by a simple governance structure, which is set up in advance and adaptable as necessary.[22] It should be maintained throughout the life of the digitalisation programme. It would therefore be advisable to fully integrate the governance structure into the body responsible for the court administration. However the governance structure is constituted, its management should have a sufficiently significant level of experience of project management and IT experience to be able to oversee the design, implementation, and ongoing governance of the digitalisation of civil justice. Its membership should also be consistent with Principle 10.[23]

2. The governance structure should be fully accountable to an appropriate State organ, eg the judiciary, the executive and/or the legislature. It should, at the least: provide a clear and effective vision of the digitalisation project, including its aims, purposes and goals; ensure that there is an effective strategy for design and implementation, including clear processes, guidelines, timelines for each part of the project and the incorporation of necessary steps to mitigate any risks that digitalisation may pose to fundamental rights and values, particularly judicial independence and equal access to justice; and make provision for the

[22] CEPEJ (2016) at 72; A McAfee, *Mastering the Three Worlds of Information Technology*, Harvard Business Review November 2006 (11), 141-149 <https://hbr.org/archive-toc/BR0611>.

[23] CCJE (2023) at [92(iv)]. Integration of the judiciary into the governance of any digitalisation project is likely to require reform to current approaches to judicial engagement in IT Governance in many European jurisdictions, see CEPEJ, *European judicial systems - CEPEJ Evaluation Report*, (2022), Part 1. See further CCJE, *Compilation of Responses for Opinion 14*, (2011) and CCJE, *Compilation of Responses for Opinion 26* (2023).

effective management for the project, including clear lines of responsibility and accountability for project teams.[24] Risk assessments should be carried out throughout the life of the project. These should include assessments of risk to judicial independence, access to justice and to other fundamental rights, as well as data sovereignty, protection and security (Principle 20).

3. Effective governance of digitalisation should be embedded into the day-to-day management of the digital civil justice system to better realise the benefits, and identify problems arising from digitalisation as well as potential improvements. To facilitate this, effective mechanisms should enable the judiciary and court administration to access judicial and court performance data. Effective governance, consistent with Principle 4, requires ownership and control of this data to be exercised by the judiciary. Access to it should, particularly, help promote fair and timely service delivery, by effective resource planning, case management and hearing scheduling (Principle 7).[25]

4. Access to information should also be provided to protect and promote judicial independence.[26] It should be provided on a differential basis. Additional to the publicly available information required under Principle 7, individual judges should have access to data concerning their individual performance. Judges in leadership roles, whether that be as members of a Judicial Council or otherwise, should also be provided with information relevant to that role.

Principle 9: Digital Design

1. *Civil justice systems should be designed and operated on the premise that the civil justice system will be, by default, a digital system. This requires, at the least:*

   a. *ensuring that digitalisation is implemented in stages sufficient to maximise the prospect of the successful implementation of the overall digitalisation programme;*

   b. *automating routine judicial and administrative tasks and processes, including case management, with reference to human intervention and decision-making where that is necessary due to the nature of the task or process;*

   c. *creating and maintaining simple and effective digital access to the civil justice system, including through the appropriate provision of accessible and reliable AI-based assistance for parties to proceedings;*

   d. *creating and managing a single digital case file for each proceeding to facilitate digital filing and management of disputes and digital access for parties. The file should also be available to any court which has a legitimate reason to access it;*

   e. *using digital communication methods between parties, lawyers, the court and the judiciary and other participants in proceedings;*

[24] K Šipulová et al, '*Judicial Self-Governance Index: Towards Better Understanding of the Role of Judges in Governing the Judiciary* (2023) 17 Regulation & Governance 22.

[25] AD (Dory) Reiling & F Contini, *E-Justice Platforms: Challenges for Judicial Governance*, (2022) 13 International Journal for Court Administration 6.

[26] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (EU GDPR)), Article 23(1)(f).

f. using digital means for the effective court-based case management of proceedings, including methods of service, and for the conduct of, and participation, in hearings by all participants in proceedings, the media and the public in general;

g. providing digital access to legal information by the judiciary and court administration; and

h. creating and using machine-readable digital judgments and other decisions that should be made available online consistently with Principle 6.

2. Digitalisation requires consideration to be given to the needs of all users. There should therefore continue to be non-digital means of access and use of the civil justice system, including the provision of assistance, where that is necessary to secure the right of equal access to justice.

Comment

1. This Principle articulates the essence of civil justice digitalisation. It emphasises that the delivery of civil justice should be carried out primarily, although not exclusively, through digitalised systems. Digitalised civil justice should be the default and standard approach. Non-digital systems and processes should, however, be maintained to the extent that they are necessary to ensure the civil justice system is fully inclusive and able, particularly, to secure equal access for vulnerable persons or those with other specific access needs (Principles 3 and 11).

2. Justice system digitalisation has been noted to be overly ambitious in some jurisdictions. Where they have focused on wholescale reform, there has been evidence of significant underestimation of the complexity of such processes, misconceptions over what is required to achieve effective implementation, and a failure to appreciate the time and costs involved.[27] Future digital-by-design programmes should minimise the risk of such problems arising by ensuring that they are incremental, iterative, and have a clearly defined purpose and clear priorities for development (Principle 16). The purposes and priorities of the digitalisation systems should give effect to Principles 2 to 7.[28] Developing priorities for staged, incremental digitalisation may, for instance, mean that digitalisation focuses initially on the introduction of e-filing, e-case management or data analytics.[29]

3. Paragraph 1 identifies key elements of any digitalisation programme, many of which have already been introduced into European civil justice systems. Where a State has not embarked on digitalisation or has only introduced limited digitalisation into their justice systems, they should consider the introduction of these elements as part of their overall digitalisation programme. Each is intended to improve access to justice and to better secure fundamental rights and values. They are also intended to improve efficiency and economy, although these aims promote access to justice and are not aims in their own right.[30] It is also important for States

[27] AD (Dory) Reiling, *Technology for Justice: How Information Technology Can Support Judicial Reform*, (Leiden University Press 2009); L Natale & A Cordella, *Digitising the Judicial Sector: A Case Study of the Dutch KEI Programme*, in R Krimmer et al, *Electronic Participation* (14th IFIP WG 8.5 International Conference, ePart 2022 Linköping, Sweden, September 6–8, 2022 Proceedings).

[28] CCJE (2023) at [81]-[89].

[29] Z Loebl, *Designing Online Courts – The Future of Justice is Open to All*, (Wolters Kluwer, 2019) at 49-51.

[30] Some countries have introduced digitalisation reforms with the aim of improving efficiency per se: see Z Loebl (2019) at 50; European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - DigitalJustice@2030* (COM (2025) 802 final) at 10. While these Principles support the promotion of efficiency, and economy through digitalisation, they see both aims as the means to achieve greater access and, hence, where they conflict with, or limit access to, justice, they should either be carefully balanced against that wider and more fundamental aim or access to justice should be given greater weight.

to learn from developments – both successes and failures – in other countries;[31] States should co-operate in this endeavour.[32]

4. The development of digital case management should follow the civil procedural code.[33] To the greatest extent consistent with Principles 2 to 7, case management should be automated by reference to the 'if this, then that' approach to coding. Exceptions to that approach should normally refer case management for judicial decision. Digitalisation of case management should facilitate data collection, including metadata, further to Principles 10, 17 and 18 and subject to Principle 20. AI assistance should be designed consistently with Principle 15.

5. Where the digitalisation of judgments is concerned, they should, at the least, include the following: an appropriate neutral case reference number (one example of which is the European Case Law Identifier); the ability for the judgment to be populated with data drawn from the case management system, eg party data, hearing data, and relevant case management events. Digital judgments may also be populated with information provided by automated summaries of case information and relevant case law, subject to review and confirmation of their accuracy by the judge responsible before the judgment is finalised. Such information may also be confirmed by the judge's digital signature (Principle 15).

Principle 10: User-Centric, Inclusive and Data-Driven Design

1. *Digital design should be user-centred and inclusive so that it can take account of the needs of all users and secure equal and effective access to the civil justice system.*

2. *To secure effective user-centred and inclusive design, digital design should be:*

   a. *based on robust, proportionate, and effective qualitative and quantitative data concerning users of the system and their respective needs;*

   b. *carried out by inclusive design teams; and*

   c. *subject to scrutiny, testing and review by users before and after implementation.*

3. *The design team should include legal, judicial, administrative and digital expertise, diversity in gender and ethnicity, and a plurality of user perspectives to ensure inclusive design.*

4. *To promote effective public scrutiny of the digital justice system, data used in the design process should, subject to Principle 20, be available publicly.*

Comment

1. *To ensure that digitalisation increases equal access to justice, it should carried out in an explicitly user-centric and inclusive manner.[34] This requires digitalisation to be*

[31] For instance, Denmark's online civil justice platform (<https://minretssag.dk/frontpage>) or the French Portalis system (<https://www.justice.fr/donnees-personnelles/portalis>; <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043771614>); Germany's OLGA system for the management of mass litigation; or, the development of the European Digital Identity Wallet as a basis for facilitating accessible, secure and differential use of digital civil justice systems (European Union, *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*).

[32] European Commission (COM (2025) 802 final).

[33] ELI/UNIDROIT (2021), r 47 to 49.

[34] Inclusivity should go further than recommended, for instance, by CEPEJ (2016) at 68, which focuses on including legal professionals in design teams.

evidence-based, drawing on qualitative and quantitative data concerning the particular needs and experiences of users of the system.[35] *In this way digitalisation can ensure that the digital civil justice system neither embeds discriminatory forms of design nor ones that result in certain categories of user being provided with less than equal access to it.*

2. *Design should, for instance, take account of the access requirements of users who have no legal training, have impaired vision or impaired hearing. It should also take account of the needs of those users with cognitive impairments, of neurodiversity, and of those users who have learning disabilities. It should not discriminate on grounds of age, race, ethnicity, sex, sexual orientation, gender or socio-economic background.*[36] *To optimise the prospect that digital design takes account of the needs of all users, it should be subject to consultation and any necessary consequential revisions before implementation commences (Principle 16).*

3. *The adequate, proportional involvement of all stakeholders in the design and maintenance of the digitalised system is necessary to ensure that it operates for the benefit of all users. While it is critically important that the judiciary and the legal profession form part of design teams,*[37] *such teams should be fully inclusive of society, ie their members should evidence a breadth of characteristics, backgrounds and experience.*

Principle 11: Public and Private Integration

To promote user-choice in effective and efficient dispute resolution, digitalisation should facilitate the integration of public, non-court-based forms of dispute resolution into the digital civil justice system. This may be achieved through:

a. *the establishment of a national website, which provides information and guidance concerning access to the digital civil justice system and non-court-based forms of dispute resolution. Access to information should include access to legislation, case law, court procedure and practices, the nature and role of dispute prevention and of non-court-based dispute resolution processes. Access should be facilitated through smart search, which may include State-provided AI that is consistent with Principle 15; and/or*

b. *the digitalisation of the civil justice system consistently with the development of data standards and interoperability as provided for in Principle 12.*

Comment

1. The vast majority of civil disputes are resolved informally outside the civil justice system with no need for assistance from, or the intervention of, any dispute resolution process. Where assistance or intervention is required, there are many different ways in which civil disputes can be resolved effectively, whether through civil proceedings before courts (public justice) or through non-court-based dispute resolution

[35] One approach that can be taken to this is through carrying out largescale, national consultation processes, such as that carried out in France as part of the planning phase of court digitalisation, see D Guillaume et al, *Digitalising Justice: A Fundamental Rights-based Approach*, (2025) at 38 <https://fra.europa.eu/sites/default/files/fra_uploads/digitalising_justice_-_country_research_-_france.pdf>.

[36] Such an approach could, for instance, see the design of court websites optimised to properly take account of these various characteristics. It could also use AI to provide automated translation or interpretation.

[37] CEPEJ, Guide*lines on How to Drive Change Towards Cyberjustice*, (2016).

processes (private justice), eg Ombudsman schemes, negotiation, early neutral evaluation, mediation, arbitration (whether binding or advisory) and various forms of online dispute resolution.

2. While the digitalisation of civil justice primarily focuses on the digitalisation of the civil courts, it provides a means to give greater effect to the approach advocated by the ELI and the European Network of the Councils for the Judiciary concerning the integration of public and private justice.[38] While there are different ways in which this aim can be achieved, this Principle recommends the adoption of either of two different approaches. It does so to promote access to justice, informed user-choice, efficiency, and systemic coherence between the two types of dispute resolution process, public and private.[39]

3. States may take different approaches to integration of public and private justice systems through digitalisation. They could create a one-stop-shop for information and access to the various different forms of dispute resolution process. This could be provided via a single national website.[40] This could help promote effective and efficient access to information about disputes, different processes through which they can be prevented, consensually resolved, or resolved through civil proceedings before courts. The provision of smart search tools and appropriate AI tools, pursuant to Principle 15, may also help increase the utility of such a website. Alternatively, States could facilitate the integration of court and non-court-based dispute resolution through the development of data standards-based interoperability that would allow existing and future providers of private, non-court dispute resolution services to align and comply with the data standards and, in that way, facilitate the automation and fair, cost-effective transfer of information about disputes between them and the digitalised civil court (see Principle 12).[41]

Principle 12: Data Standards and Interoperability

1. *Digitalisation should be designed consistently with clear, technology-neutral, and publicly available data standards.*

2. *Data standards should, at a minimum, enable the digital justice system to identify areas for improvement in its ability to secure Principles 2 to 7. They should ensure interoperability and the secure exchange of data across all parts of, and to all participants in, the digital civil justice system and other digitalised justice systems.*

3. *Data standards should also secure interoperability between the digital civil justice system and non-court-based dispute resolution providers connected with that system.*

4. *To promote effective and efficient cross-border civil justice, European states should promote the development of common publicly accessible, open, data standards to facilitate interoperability between their national digital civil justice systems.*

5. *Data standards should be developed by the digitalisation design team with input from, and in collaboration with, the court administration, judiciary, Government,*

[38] ELI-ENCJ, *Report On The Relationship Between Formal and Informal Justice: the Courts and Alternative Dispute Resolution*, (2018) at 9.
[39] J Sorabji, *A Modern Civil Procedure Code for England and Wales*, (OUP, 2024).
[40] See, for instance, the approach taken in England and Wales: G Vos MR, *The Future of Courts*, (2024) <https://www.judiciary.uk/wp-content/uploads/2024/05/UCL-The-Future-of-Courts-OPRC-DJS.pdf>. Also see the approach taken in France via <https://www.justice.fr>.
[41] M Ahmed, *A Critical Review of the Official Injury Claims Service*, (2023) 2 Journal of Personal Injury Law 130.

representatives of civil society, public and private sector providers of legal advice, assistance and dispute resolution, software designers and researchers Oversight of data standards when implemented should reside with the body responsible for digitalisation.

Comment

1. It is essential that digitalisation implements a clear, technology-neutral[42] set of data standards consistent with the promotion of Principles 2 to 7.[43] To promote transparency and accountability, these standards should be available to the public.

2. Data standards should be developed for, amongst other things, the integration of public and non-court-based dispute resolution processes through the collection of standard key case data, including information concerning disputes and the parties to them, which can then be transferred seamlessly between parties, other participants in proceedings, and different dispute resolution processes, including to the digitalised civil court (Principle 11).[44] To that latter end, it is essential that data standards to promote inclusion and system accessibility are developed. They should thus facilitate the collection of data relating to the characteristics of participants in proceedings to help promote equal, non-discriminatory access to justice, particularly for vulnerable participants or those who are disadvantaged.[45]

3. Data standards should also facilitate interoperability, where possible, between digital civil justice systems between States, an issue that is particularly important within the European Union.[46] It is also of wider importance given the growth in cross-border litigation and enforcement of judgments generally. Interoperability, moreover, should not be limited to the current state of technology. Care should be taken to ensure that digitalisation, and particularly improvements over time to the digitalised system, to take account of technological developments, eg the potential future use of quantum computing, are incorporated effectively into the system.

3. The development of data standards should be carried out by the body responsible for developing and implementing digitalisation (Principle 10). Once developed, oversight of the data standards should reside with the body responsible for digitalisation, while taking adequate account of the views of all relevant stakeholders (Principles 16 and 17).

Principle 13: Enhanced Accessibility

1. *Digitalisation should enhance equal access to justice for all citizens and the State's ability to promote public justice. It should do so through enhancing access to the civil justice system by providing:*

---

[42] This Principle emphasises the point that information technology continues to develop significantly. The protocols and data standards should therefore be prepared so that they are not particular to any specific technology or form of technology. Hence, while application programming interfaces (APIs) are typical means by which data standards can be implemented, they may not be in the future.

[43] Examples of court data standards, include: His Majesty's Courts and Tribunals Service (UK), *Civil Bulk Upload Service (CBUS) - CNBC Customer Interface Definition*, <https://assets.publishing.service.gov.uk/media/686f9c602557debd867cbf44/Civil_Bulk_Upload_Service_-_Data_Standard_example.pdf>; National Center for State Courts, *National Open Court Data Standards*, <https://www.ncsc.org/our-centers-projects/national-open-court-data-standards>; European Legalisation Identified <https://eur-lex.europa.eu/eli-register/what_is_eli.html>; European Case Law Identifier <https://webgate.ec.europa.eu/e-justice/175/EN/european_case_law_identifier_ecli>.

[44] This can enable key information such as that contained in letters of claim and reply, documents, stocktake reports that narrow issues in dispute, negotiation histories, mediator summaries, or process metadata to be made available between non-court-based dispute resolution providers and digitalised civil courts in a structured, machine-readable form. This reduces duplication, cost, and delay.

[45] See for instance, Online Procedure Rule Committee, *Inclusion Framework and Pre-Action Model for the Digital Justice System*, (2025). For analogous approaches to data standards concerning security standards, see for instance, ISO 20022, which provides a '*single standardisation approach (methodology, process, repository) to be used by all financial standards initiatives*' <https://www.iso20022.org/about-iso-20022>.

[46] See, for instance, European Commission, (COM (2025) 802 final).

a. access to the digital civil justice system for all users in a state's official languages as well as through the provision of translation tools to facilitate translation into other languages;

b. digital access to public legal aid and assistance, including digital legal diagnostic tools for the guidance of individuals who do not have access to legal advice or assistance from a regulated legal professional;

c. access via a range of digital communication channels, including mobile and website access, for communication between participants and other participants in proceedings (including potential proceedings) and participants and the court;

d. facilities to digitally initiate and defend proceedings, file, access and manage documents and other information, and, where appropriate, participate in domestic and cross-border proceedings, including hearings, and to pay applicable court fees;

e. the means to verify digitally the identity of participants in proceedings, particularly parties and their legal representatives, as needed;

f. secure means through which live streaming hearings, digital hearings, and hearings using other forms of technology may take place fairly and effectively, including through the provision of reliable internet connectivity;

g. the means by which parties to proceedings and their legal representatives can access hearings digitally in a secure manner so they may present their arguments freely and, where necessary and legally appropriate, privately and with respect to the confidentiality of their communication;

h. effective forms of digital enforcement procedures and measures, including facilities to access advice and assistance concerning enforcement and enforcement professionals; and

i. digital public access to public court documents, including public aspects of court files, judgments and orders. Access to judgments and decisions should be consistent with Principle 6 and should be provided free of charge. Where necessary and legally appropriate, access to other documents may be provided.

2. To ensure the effective use of digital communication, use of such channels should be mandatory for all regulated legal professionals, other professional court users and companies.

3. Any non-digital communications should, in so far as possible, be converted by the court administration into a digitalised format to enable them to be processed through the digital civil justice system.

Comment

1. Digital technology should promote effective and equal access to justice and public justice (Principle 3 and 6). This Principle provides guidance on how they can be promoted in the digital context.

2. Paragraph 1 makes clear that digital access encompasses the provision of a wide range of information that can promote access to justice, eg access to legal aid and assistance,[47] to court-fees payment systems, court files, relevant court

[47] The right to legal aid is an integral part of the right to fair trial: Article 6 ECHR, art 47(3) EU Charter; *Airey v Ireland* (1979) 2 EHRR 305 at [26].

documents, hearings, enforcement proceedings and public court judgments. Provision of information concerning legal assistance is particularly beneficial prior to court procedures being initiated. It can, for instance, provide helpful access to information concerning non-court-based dispute resolution processes, access to legislation and court judgments, as well as information on how to access legal services, including legal aid provision. Such information is essential in securing effective access to justice.[48] It can be made available through judicial or court websites.[49] This help may also be made available through other publicly available digital means or, where appropriate, legal helpdesks.[50] In cross-border cases, digital access to pay court fees and to court information, both of which may be facilitated through the use of AI language translation tools as well as via online payment and information systems, is particularly important.[51]

3. Paragraph 1 also emphasises how digitalisation enhances accessibility through enabling proceedings to be initiated and defended through dedicated secured web portals or otherwise. These portals should be accessible to parties and/or their representatives and should secure authenticity, integrity, and confidentiality. This includes measures to verify the identity of parties, witnesses and representatives. It also makes provision for digital access to hearings, subject to data protection requirements (Principle 20). It also clarifies that the right of access extends to enforcement procedures, in respect of which digital technology can support timely and less burdensome enforcement.[52] Paragraph 1 encompasses all competent enforcement authorities, including courts, judicial officers, bailiffs, notaries and other public enforcement agencies. Where mobile access is being considered, specific care should be taken to implement it at proportionate cost and consistently with effective data security requirements (Principles 19 and 20).

4. Paragraph 2 emphasises how digital communication with the court is mandatory for legal professionals, other professional court users (eg expert witnesses, enforcement officers), and companies where they are not represented by legal professionals. Parties who are not represented by legal professionals and non-professional court users who have limited digital capacity are not required to use digital communication channels, although they should be encouraged to do so where they can. As digital communication for these parties is also beneficial to further access to justice, its use should be supported by providing necessary practical and technical assistance (Principles 3 and 9).

5. Paragraph 3 is intended to promote the efficacy of the digital civil justice system through requiring, insofar as that is possible, non-digital information provided to the court to be included in the digital case file. This applies whether non-digital information was provided due to the nature of the information (eg physical evidence) or due to the use of non-digital communication by a party. This secures court and party access to all information in the case. Proper working practices with both the content data and the metadata being collected through the communication, need to support automating the case management to the greatest possible extent.

---

[48] J Hoevenaars & X E Kramer, *Improving Access to Information in European Civil Justice: a Mission (Im)Possible?*, in J von Hein & T Kruger (eds), *Informed Choices in Cross-Border Enforcement*, (Intersentia, 2020), at 503-525; L E Mitee, *The Right of Public Access to Legal Information: A Proposal for its Universal Recognition as a Human Right*, *German Law Journal* 2021, 1429.

[49] See, for instance, in the Netherlands www.rechtspraak.nl, which provides among others information on courts, procedures, court fees and case law, and information provided in the United Kingdom www.judiciary.uk and in Romania https://portal.just.ro/SitePages/ghid.aspx. In the EU, the European e-Justice Portal https://e-justice.europa.eu provides extensive information on relevant (EU) legislation, court procedures, case law, registers and legal professionals.

[50] For instance, the European Consumer Centre's national contact points.

[51] On the payment of fees in the EU see, Article 9 Regulation (EU) 2023/2844 on digitalisation of judicial cooperation in the EU context.

[52] CEPEJ, *Guide on Judicial E-Auctions*, (2023).

Principle 14: Enhanced Transparency and Accountability

1. *To increase transparency and public accountability of the civil justice system, digitalisation should, subject to any legitimate legal derogations or limitations, incorporate the following:*

   a. *enhanced public, including media, access to court listings via court websites in addition to their provision in court buildings;*

   b. *for hearings via digital means or by hybrid means where some participants are in court and others take part via digital means, information should be provided about how the public, including the media, can access the hearing on an equivalent basis to that which they could access if they attended the hearing if it was held in court, including concerning provision of documents during a hearing;*

   c. *access to the digital court file by the public for legitimate reasons;*

   d. *automated translation and interpretation systems may be used to secure effective participation of parties in, and public access to, proceedings;*

   e. *livestreaming or broadcasting hearings;*

   f. *hearings, both in court and online, should be recorded and transcribed digitally. Where possible, transcriptions should be made in real-time. Transcriptions should be retained in a machine-readable format;*

   g. *access to recordings and transcriptions, and where appropriate AI-generated plain language summaries of transcriptions, should be accessible to the court and parties to the proceedings and those who have a legitimate legal interest in accessing them; and*

   h. *publication of judgments and other court documents in a machine-readable format on free-to-access digital national databases maintained by a judicial or other public authority.*

2. *Information should also be made available to participants in proceedings and the public in general concerning the operation of the digital civil justice system, including general statistical and other data concerning the number of proceedings, types of claim, the length of proceedings, settlement and judgment rates.*

Comment

1. This Principle articulates how digitalisation can further the right to public justice (Principles 4 and 6). Digitalisation can, for instance, increase public access to civil proceedings through free-to-access provision of advance online information on a digitalised civil court's website or other official website concerning court hearings. This could provide information concerning: the nature of the dispute; a short statement of facts, the procedural history of the proceedings and, where appropriate and legal, parties' written submissions,[53] the names of the parties; the type of hearing that is scheduled; the name of the judge(s) who is to manage the proceedings or conduct a hearing or the mode of the hearing. Where a hearing is to be held remotely, information can also be provided as to how it can be accessed. Such information should be accessible, easily understandable, and

[53] See, for instance, the approaches taken by the European Court of Human Rights <https://www.echr.coe.int/calendar-of-hearings>; UK Supreme Court <https://www.supremecourt.uk/cases> and that taken in Spain via the Judicial Electronica – Sinage Service <https://sedejudicial.justicia.es/en/inicio>; and in The Netherlands via the Rechtspraak <https://www.rechtspraak.nl/Naar-de-rechter>.

in a format that allows for effective search and filtering of results.

2. Digitalisation ought to improve the public's access to individual court case files where they have a legitimate legal interest in obtaining access to the information contained in it, eg where access is necessary for a party to the proceedings or potential proceedings to obtain information that is relevant to their own case. Access need not, however, be given to internal court administrative information held on a digital case file or to information that would infringe judicial independence, the integrity of proceedings or the administration of justice.

3. The use of both automated translation and interpretation systems addresses the issues of both party participation and effective access by the public to civil justice systems. Language barriers can significantly impede a party's ability to engage fully and on a non-discriminatory basis in court proceedings. Automated translation systems allow parties who do not speak the court's official language or languages to understand statements of case, procedural directions and evidence. It enables them to participate effectively in hearings, including making oral submissions, thus promoting not only accuracy in decision-making by the court but also securing a greater sense of procedural justice for the party. For the public, media and other non-parties to the proceedings (eg researchers), automated translations can make proceedings more accessible and understandable. The same points can properly be made in for interpretation services.

4. Making provision for the broadcasting or livestreaming of hearings is a further means to improve transparency and accountability, as well as equal and effective access to justice. Technological mechanisms and legal measures should, however, be put in place to protect the administration of justice and other fundamental rights and values, including that of data protection, from unauthorised further broadcasting or publication.[54] Legal measures include provision of criminal sanctions such as those that apply where there is an unlawful interference with the administration of justice (Principle 20).

5. Digital hearing transcriptions and recordings can also enhance transparency, accountability, and access.[55] Real-time transcription improves accessibility for the parties to the proceedings, the public and the media. They can provide an authoritative record for any appeal. Storing transcriptions in machine-readable formats further allows efficient search and analysis and supports both procedural fairness and broader oversight of the civil justice system through legitimate non-party access to them. Principles 2 to 6 can also be promoted through: the use of court-approved, accurate AI-generated plain language summaries, which can make complex factual and legal issues understandable; and making all judgments and other court decisions available from a free-to-access single, national digital platform.[56]

6. Paragraph 1 stresses that measures taken to enhance transparency and accountability provided further to this Principle may need to be limited where that is required for a legitimate legal reason, eg where redaction may be

[54] See the Court of Appeal (Civil Division) (England and Wales)'s YouTube page <https://www.judiciary.uk/the-court-of-appeal-civil-division-live-streaming-of-court-hearings/>.

[55] See the automated transcription of proceedings in Estonia (Digitalisation Regulation (Regulation (EU) 2023/2844) – by Estonia concerning sec 159 <https://e-justice.europa.eu/topics/court-procedures/digitalisation-regulation-member-state-notifications/ee_en>.

[56] See: Italy's ItalgiureWeb, which is managed by the Electronic Documentation Centre of the Supreme Court <www.italgiure.giustizia.it> and SentenzeWeb <www.italgiure.giustizia.it/sncass>; England and Wales' National Archive's Find Case law database <https://caselaw.nationalarchives.gov.uk/search/advanced> and the UK Supreme Court's database <https://www.supremecourt.uk/cases>. Also see CEPEJ, *Guidelines on videoconferencing in judicial proceedings*, (2021), Parts 1 and 12 <https://edoc.coe.int/en/efficiency-of-justice/10706-guidelines-on-videoconferencing-in-judicial-proceedings.html#>; European Commission, EU Justice Scoreboard 2023 at 36 <https://commission.europa.eu/system/files/2023-06/Justice%20Scoreboard%202023_0.pdf>.

justified, where transparency may frustrate the court's ability to do justice, or to protect a public interest, such as national security, privacy and other fundamental rights (Principle 6).[57] Examples of limitations may include: redaction or anonymisation of the parties, witnesses or judges to the extent provided by national law and/or required to give effect to fundamental rights and values (Principles 2 and 6); digital hearing schedules only made available online for a period necessary to promote public access to a hearing so as to strike an effective balance between the right to public justice and data protection and privacy rights; and ensuring that judges are provided with effective technology-based access controls where hearings take place via a digital platform so that they may control public access on an equivalent basis to that of a hearing in a physical court building.

7. Paragraph 2 highlights the importance of making information, eg general statistical data, concerning the operation of the digital civil justice system publicly available in an accessible and user-friendly manner.[58] This not only improves transparency and public accountability, but also helps facilitate the effective evaluation of the system's operation (Principle 17).

Principle 15: Artificial Intelligence

1. *AI tools should be incorporated and used, as appropriate, throughout the civil justice system. Particular care should be taken to ensure that any form of AI incorporated into, or used in, the civil justice system is free from bias, is transparent and intelligible, and subject to appropriate accountability and human oversight. The design and use of such AI tools should also be ethical and consistent with good practice guidance.*

2. *The judiciary should only use AI to assist the administration of justice, which includes its use to assist their management of, and decision-making in, proceedings. It should not generally be used to replace judicial decision-making. Provision may, however, be made for parties to individual disputes to agree to the use of automated decision-making by AI where such consent is freely and expressly given on a fully-informed basis.*

3. *Court administrators may use AI to assist with the efficient management of court resources, including resource allocation within the civil justice system, consistently with Principles 2 to 5.*

4. *The judiciary and court administrators should be given training in the appropriate use of AI and placed under a specific obligation to ensure that they use AI judiciously. They should be individually responsible for ensuring the reliability and accuracy of any AI work-product they utilise. They should receive training on a regular basis on the safe and appropriate use of AI.*

Comment

1. The use of AI tools in a digital civil justice system is expected to yield significant benefits. It can, for instance, improve efficient and economical case management, including scheduling hearings, assist with legal research, help identify facts and analyse evidence, and summarise documents. The use of AI is expected to improve the quality of justice by, for instance, increasing

[57] Article 6 ECHR; *Zagorodnikov v Russia* - 66941/01 [2007] ECHR 457 at [26]; *B and P v the United Kingdom*, no. 36536/97, (ECHR, 24 April 2001) at [38]–[39]; *Osinger v Austria* - 54645/00 [2005] ECHR 183 at [45].

[58] See N Byrom, *Digital Justice: HMCTS data strategy and delivering access to justice Report and recommendations*, (The Legal Education Foundation, 2019) at 2 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835778/DigitalJusticeFINAL.PDF>. Also see the approach taken by CEPEJ on the publication of such data.

the prospect that like cases will be treated alike and different cases will be treated differently.[59] Its use by courts and judiciaries is, however, identified as a high risk.[60] It is essential therefore that design and use of AI within the digital civil justice system should be consistent with accepted good practice.

2. Examples of good practice are provided in: the Council of Europe's *Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law*;[61] the Council of Europe's Consultative Council of European Judges' *Opinion No. 26*;[62] and, CEPEJ's *Guidelines On The Use of Generative Artificial Intelligence For Courts*;[63] and, the *ELI-Mount Scopus International Standards of Judicial Independence* (2024).[64] Good practice particularly requires AI incorporated into the digital civil justice system and used by the judiciary and court administrators to respect fundamental rights, democracy and the rule of law fully. Steps should be taken to ensure that its design and operation is free of bias, compatible with the principle of non-discrimination, uses certified sources and is transparent and intelligible. It should remain subject to human control, oversight and verification, particularly in respect of the results of its use.[65] To ensure appropriate and responsible use, judges and court administrators should be given training and official guidance on the use of AI.[66] Effective risk management and data governance management practices should also be implemented to ensure that AI is only used for its authorised and intended purpose, as defined by prescribed rules.[67]

3. Digitalisation and the incorporation of AI into the civil justice system should ensure that the ultimate responsibility for judicial decisions remain with humans. AI should support rather than supersede judges.[68] Automated decision-making through the use of AI is, however, permissible where parties to a dispute explicitly and freely agree to its use on an informed basis. Where such automated decision-making is used, it should be subject to such safeguards as apply to human decision-making.[69]

---

[59] CEPEJ, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, (2018), Principle 5; ELI, *ELI-Mount Scopus International Standards of Judicial Independence*, (2024), Standard 23(c).

[60] EU AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828).

[61] Council of Europe, *Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law*, (2024).

[62] CCJE (2023).

[63] CEPEJ, *Guidelines on the Use of Generative Artificial Intelligence for Courts*, (2025). Also see, CEPEJ, *Use of Generative Artificial Intelligence (AI) by judicial professionals in a work-related context*, (2024).

[64] ELI-Mount Scopus (2024), standard 23.

[65] ELI-Mount Scopus (2024).

[66] See *Artificial Intelligence, Guidance for Judicial Officers*, (2025, England and Wales) <https://www.judiciary.uk/wp-content/uploads/2025/10/Artificial-Intelligence-AI-Guidance-for-Judicial-Office-Holders-2.pdf>.

[67] ELI-Mount Scopus (2024), standard 23(d); EU AI Act; AD (Dory) Reiling, *Courts and Artificial Intelligence*, (2020) 11 International Journal for Court Administration 8.

[68] CCJE (2023) at [92(iii)].

[69] ELI-Mount Scopus (2024), standard 23 (e). The design and use of automated decision-making should be carried out consistently with ELI, *Guiding Principles for Automated Decision-Making in the EU*, (2022).

Part III – Implementation and Operational Principles

Principle 16: Iterative Evolution and Piloting

Digitalisation is a continuing process. It should follow good practice, including: investment in people; appropriate responsibility and accountability mechanisms; clarity of purpose; effective early user testing; piloting and iterative development; and, where appropriate, continuous improvement and iterative evolution.

Comment

1. Digitalisation of civil justice needs to be a continuous process given the rapid development of information technology and AI in particular. It should be carried out consistently with a clear purpose, as set out in Principles 2 and 9. It requires frequent updating and revision to take account of technological advances, not least emergent threats to the system's safety and integrity so as to ensure that it remains a publicly accessible system (Principle 20). This will also require sustainable resourcing (Principle 19).

2. Iterative evolution and piloting are key mechanisms to maximise the prospect that digitalisation will be designed and implemented successfully. They minimise the risk of implementation failure or that digitalisation programmes will need to be scaled back during implementation.[70] Giving effect to these mechanisms requires digitalisation to be carried out consistently with accepted good digital transformation processes including:

- **Investing in people**. Individuals with high levels of skill and experience in the successful delivery of digitalisation programmes should be appointed by the body responsible for digitalisation of civil justice. These should include project managements and technical staff. Investing in people should also include training existing court administrators and judges. To facilitate effective investment in people, an experienced Chief Digital Officer should be appointed to the state body responsible for court administration and, where that is not the judiciary, the judiciary. They should have overall responsibility for the delivery of the digitalisation programme (Principles 9 and 10);

- **Early user testing and piloting**. Digital processes should be subject to early user testing. It should be understood that developments may fail to achieve their objectives, which may lead to specific pilot schemes being abandoned or revised in the light of lessons learnt.[71] Beta testing or the use of digital sandboxes, ie secure test environments through which innovative digital procedures can be developed, should be utilised. User testing should be carried out consistently with Principle 10;

---

[70] K Oh et al, *Determinants for Successful Digital Transformation*, Sustainability 2022, 14, 1215 <https://doi.org/10.3390/su14031215>; N Ramesh & D Delen, *Digital Transformation: How to Beat the 90% Failure Rate?*, IEEE DOI 10.1109/EMR.2021.3070139; S Cowlishaw, *Digital court system E-Bench's failure leads to near $7 million write-off*, (Dominion Post, 21 April 2015) <http://www.stuff.co.nz/dominion-post/news/politics/67918645/Digital-court-system-E-Benchs-failure-leads-to-near-7-million-write-off>; L Natale & A Cordella, (2022) at 146; N. Goodwin, *Update on the HMCTS Reform Programme*, (Letter to Sir Geoffrey Clifton-Brown MP, Chair of the Public Accounts Committee, 13 February 2025) <https://committees.parliament.uk/publications/46829/documents/240988/default/>; AD Reiling, *Technology for Justice, How Information Technology can support Judicial Reform*, Leiden University Press 2009. AD (Dory) Reiling & F Contini, (2022).

[71] See CEPEJ (2016) at 69.

- **Effective collaboration**. The body responsible for digitalisation should collaborate with legal non-governmental organisations (NGOs), the legal profession and other professional users of the civil justice system. This should be carried out to maximise the prospect that digitalisation will complement and be interoperable with digital systems used by the legal profession and those other professional users. To promote the integration of non-court-based dispute resolution with the digital civil justice system, as wide a range of providers of such processes as possible should also be engaged in the design process. Collaboration with universities, legal advice organisations, and Law Tech innovators to establish and fund Judicial TechLabs,[72] which can provide a focus for longer-term research and development in digital technology for use in the digital justice system, should also be carried out. Collaboration with digitalisation initiatives in other countries would also be beneficial;

- **Use of agile processes**. Design and its implementation should be iterative. It should look to build-in improvement particularly through seeking and taking account of user-feedback drawn from all users and appropriate qualitative and quantitative research.[73] Building improvement during the digitalisation programme should include both improvements to discrete digital processes and expansion of the digitalisation programme in consistently with Principle 9.

Principle 17: Evaluation

1. *Effective evaluation is an essential feature of any civil justice system that seeks to give effect to Principles 2 to 7. It is required at a systemic level and an individual level. It should be carried out by the state body responsible for court administration and, where that is not the judiciary, the judiciary.*

2. *Systemic evaluation assesses the extent to which the digital civil justice system as a whole is able to secure fair, efficient, cost-effective access to civil justice. Individual evaluation assesses whether individual judges are managing and disposing of individual proceedings through using the digital system in a fair, cost-effective and efficient manner.*

3. *The digital civil justice system should provide the means to capture and assess both quantitative and qualitative data, including from feedback from participants in proceedings and the public in general, that facilitate both systemic and individual evaluation.*

4. *Evaluative data should be used to consider what improvements or modifications may need to be implemented to the digital civil justice system as a whole, in accordance with Principle 13. Where individual evaluation is concerned, the judiciary and court administration should use evaluation data to improve the management of proceedings.*

Comment

1. Effective evaluation of digitalisation is necessary to determine whether it achieves its objectives, the extent to which it does so, and if not, why not. This is particularly important where digitalisation seeks to improve equal access to justice for disadvantaged individuals or groups. Evaluation must also identify unintended adverse consequences of digitalisation or novel problems, including those arising from external

[72] J Barnett et al, *JudicialTech supporting Justice - The impact of AI and Emerging Technologies on the Judiciary, Courts and Justice* (2025) at 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241272>.

[73] R Koulu & J Hakkarainen, *Law and digitalisation: Rethinking Legal Services*, (University of Helsinki Legal Tech Lab, 2018) at 95 <https://helda.helsinki.fi/server/api/core/bitstreams/223af371-e376-4e37-b708-321bcdd4abcd/content>. See further, The Association of Project Management <https://www.apm.org.uk/resources/find-a-resource/agile-project-management/>.

developments, eg changes in substantive law, societal change or the growth of specific types of litigation. Evaluation should therefore be an ongoing process and digitalisation cost.

2. The value of systemic evaluation of the justice system as a whole has long been recognised.[74] It requires the collection of quantitative data from the digitalised justice system, including that on the speed of proceedings, cost of resolution, and patterns of use. It should be facilitated through the use of key performance indicators.[75] The use of qualitative data, for instance concerning user experience and barriers to access (whether actual or perceived) is equally important. Together, these data should inform continuous improvement of the system (Principle 14).

3. Systemic evaluation also enables broader scrutiny of the nature and types of disputes which enter the digital justice system. Analysis of this data may illuminate patterns of recurring disputes, which may inform legislative reform or the development of new non-court-based dispute resolution schemes. This may help prevent future potential disputes in such areas arising or being capable of early resolution.

4. Finally, evaluation should also operate at an individual level. The digital justice system should therefore incorporate the means to access how effectively it is used in individual disputes. This can enable judicial leadership (a relevant Court President or Judicial Council) to identify judicial training needs or support. To maintain judicial independence, evaluative data used in this process, which is not anonymised, should remain confidential.

Principle 18: Effective Training and Guidance

1. *To fully realise the benefits of digitalisation, the judiciary and court administration should receive effective guidance and training on the nature and use of technology. Training should be refreshed regularly, and specifically when further digitalisation is effected.*

2. *Guidance should also be provided for court users to improve their ability to access the digital justice system.*

Comment

1. To utilise digital systems effectively, States should ensure that sufficient and appropriate guidance and training on the nature and use of technology is provided to the judiciary and court administration. This is necessary to enable them to contribute effectively to the design, implementation, and ongoing evaluation of digital systems.[76] In this regard it is particularly important that the judiciary generally, and those members of the judiciary specifically who are involved in the digital design and implementation process and those who have oversight of it at a senior level, are IT-literate.[77] The provision of guidance and training is also essential to enable digitalised systems to be operated effectively by the judiciary and court administration.[78]

2. Provision of any necessary training will inevitably raise resource questions and will need to be factored into the provision of sustainable

[74] J Kakalik et al, *Just, Speedy and Inexpensive? An Evaluation of Judicial case Management under the Civil Justice Reform Act*, Rand Institute for Civil Justice (1996).

[75] Typical KPIs include: length of the proceedings, number of incoming and resolved cases, clearance rate and disposition time, court room utilisation rates, etc. CEPEJ, *Time Management Checklist*, (2023); CEPEJ, *Revised Saturn Guidelines For Judicial Time Management* (3rd Revision).

[76] On the importance of such training, see, for instance, European Commission, *European Judicial Training Strategy 2025 – 2030 - Creating a supportive environment for DigitalJustice@2030*, (COM(2025) 801 final).

[77] On comparable approaches in the field of administration and management, see T Bunjevac, *Judicial Self-Governance in the New Millennium*, (Springer, 2020) at 51.

[78] CCJE, (2023) at [72], [76] and [92(xiv)].

funding for the digital justice system (Principle 19). This is a particularly important factor for States to consider for two reasons. First, the inter-relation between guidance, training and funding should be taken account of due to digitalisation being an ongoing process. As digital systems are improved and upgraded to take account of technological developments, new training and guidance needs will arise and will need to be funded. Secondly, even when digital systems are in steady state, there is an ongoing need for regular training and guidance. This is required for new members of the judiciary and court administration. Existing members should also be provided with regular refresher training, an issue which is particularly important in matters such as data and privacy protection.

3. Where the use of AI is concerned, it is essential that the judiciary and court administration are given guidance on its proper, lawful and effective use, and the potential harm to the integrity of the justice system through inappropriate use or misuse. Such training should be mandatory.[79]

4. To increase equal access to justice, guidance should also be provided to users of the digital justice system on how to access it effectively. It should be provided through both digital and non-digital channels. The latter may, for instance, include in-person guidance provided in court or other public buildings or via free legal advice services. Guidance may also be provided through telephone advice services provided by the court administration. Both digital and non-digital guidance should be designed consistently with Principle 10.

Principle 19: Sustainable Funding

1. *Digitalisation requires the commitment of adequate financial resources for its effective design and implementation. Those resources should be provided on an on-going basis to secure the effective maintenance, updating and, where appropriate, improvement of the digital civil justice system.*

2. *Digitalisation should not primarily be considered as a means to reduce State expenditure on the civil justice system. While it may help to increase court and judicial efficiency and the more economical delivery of civil justice, that should not justify a reduction in funding for the system below that required to give effect to the obligation to secure effective design and implementation of digitalisation.*

Comment

1. The right to a fair trial requires States to organise their civil courts so they can guarantee the right to a final decision on the merits of disputes and effective enforcement within a reasonable time.[80] This requires States to provide adequate levels of funding for their civil courts and the judiciary to enable them to render this right practical and effective. Furthermore, the provision of such funding should be consistent with the principle of judicial independence.[81] Digitalisation should be carried out consistently with these requirements. It should thus be supported by ongoing, adequate, sustainable funding.[82] This includes funding: to design, implement and upgrade digitalisation; and to secure necessary training required for court administrators and judges to enable them to operate the digitalised

[79] UNESCO, *Guidelines on the use of AI Systems in Courts and Tribunals*, (2025) at 23-26.
[80] *Frydlender v France* [2000] ECHR 353 at [45]; *Hornsby v Greece* (1997) 24 EHRR 250 at [40].
[81] CCJE, *On the Funding and Management of Courts with Reference to the Efficiency of the Judiciary and to article 6 of the European Convention on Human Rights*, (Opinion No 2 of 2001).
[82] R Susskind, *Online Courts and the Future of Justice*, (OUP, 2019) at 84-85.

system effectively. It also requires the State to ensure that effective systems are in place to manage the funding provided for digitalisation prudently. Effective planning and governance of the use of funding is thus necessary (Principle 8). Budgeting and external scrutiny of the use of funding should also be established (Principles 14 and 17). Accountability mechanisms should be put in place to promote good practice in budgeting, planning and resource use. These measures should, however, not compromise judicial independence (Principle 4).

2. Digitalisation, if carried out effectively, should improve the civil justice system's operation. It ought to promote administrative efficiency, economy, and increased productivity. That it ought to secure these benefits should not, however, be taken to entail a reduction in state expenditure on the civil courts and the judiciary.[83] IT funding should be based on its contribution to improve court performance, the quality of justice and the level of service to citizens.[84] While digitalisation may ultimately produce operational cost savings,[85] it should be understood that it does not necessarily, and often does not, do so.[86] IT provision, maintenance, effective operation and improvements come at a cost, which may well outweigh any efficiency or productivity-based cost savings. Given this, it is essential that States implement this Principle properly, not least due to the risk that a failure to maintain a digitalised system poses to data security, system integrity and, hence effective access to justice.

Principle 20: Digital Sovereignty, Data Protection and Security

1. *States should implement effective measures to secure digital sovereignty regarding the digital civil justice system, including its infrastructure and data held within it. Measures should also be implemented to secure effective and proportionate data protection and security. These should include such technical and organisational measures necessary to maintain system integrity and give effect to Principles 2 to 7.*

2. *Data protection and data security should be consistent with the implementation of differential access to different types of information. This, particularly, requires the introduction and maintenance of mechanisms that permit differential access to different participants in proceedings, court administration, the judiciary, the public and the media. Differential access should, particularly, protect the confidentiality and legally privileged nature of any data processed by the digital civil justice system.*

3. *Unauthorised access to, or processing of, data held within the digital civil justice system should be punishable as an interference with the administration of justice as provided for in national law.*

4. *Back-up systems should be established to mitigate against the risk of technical failure and maintain the capacity of the digital civil justice system to operate effectively and maintain the safety and integrity of data within it.*

[83] CCJE (2023) at [75]-[76].
[84] CCJE (2011) at [41].
[85] European Commission (COM (2025) 802 final).
[86] L Natale & A Cordella, (2022) at 146.

5. *The digital civil justice system should have dedicated officers responsible for the implementation and maintenance of the technical and organisational measures required to provide effective data sovereignty, protection, and security.*

6. *To provide an effective means to scrutinise the implementation and maintenance of digital sovereignty, data protection and security, States should provide the means for the judiciary to establish a Digital Court Data Authority, which should be functionally independent of the courts and judiciary. It should, consistently with the need to respect judicial independence, be capable of providing guidance to civil courts and the judiciary on data sovereignty, protection and security issues concerning the digital civil justice system. The Digital Court Data Authority should also be able to respond to complaints concerning such matters and be able to award compensation in appropriate circumstances. Where necessary, it should consult any national Data Protection Authority.*

Comment

1. The civil justice system is one of the means through which the judicial power of the State is exercised to resolve disputes concerning individuals, businesses, and the State fairly and according to law. This requires the processing, both administratively and judicially, of significant amounts of personal and other information provided by, and concerning, judges, litigants, lawyers, expert and other witnesses and a wide range of others. This includes: sensitive personal data protected by data protection law, including that of minors; sensitive business and commercial information; sensitive information concerning national security; confidential information of various types; and information that is, or may be, subject to legal professional privilege.

2. It is, therefore, of paramount importance that states retain sovereignty over their digitalised civil justice systems, their infrastructure and the data processed by them. Due to the increasing reliance by states on information technology provided by private enterprises, including ones that are under foreign jurisdiction, questions of sovereignty over digitalised justice systems are likely to become more acute over time. It is therefore incumbent on those responsible for digitalisation to ensure that the State body responsible for the civil justice system retains full legal and practical control over the digitalised system, particularly its infrastructure: digital sovereignty should be embedded in digitalisation.

3. It is also necessary for digitalisation to give effect to data protection and security requirements and, in that way, also ensure that fundamental rights, not least those to access to justice, privacy and data protection are respected. To give effect to data sovereignty, protection and security, appropriate legal, technical, and organisational measures should be incorporated at the design stage of any digitalisation process. They should then be incorporated into the digital civil justice system through the digitalisation process, maintained and made subject to regular review and, where necessary, updating. Where necessary, to protect data sovereignty, legislation may be necessary to protect it and, for instance, obviate the potential for digitalisation to result in the creation or maintenance of any infrastructure or operational dependency on third-country technology, services, or businesses. Where data protection and security are concerned, organisational measures should also ensure that those responsible for administering the digital civil justice system do so consistently with data protection and data security requirements.

4. A range of technical measures can be taken to secure effective data protection. These include: data protection impact assessments; regular data protection and data security training; the use of high levels of data security, including where

appropriate, encryption of data, consistent with international standards,[87] and differential access controls to information held within the digital civil justice system;[88] regular data protection and security audits and, where necessary, updating and upgrading of data protection and data security measures, not least to maintain the effective functionality of the civil justice system as part of the State's critical infrastructure.[89] This should particularly be done to respond to developments in data protection law, evolving technological developments, and emerging data security threats. Back-up systems should also be established to ensure continuity of access to, and use of, data held in the digital civil justice system at any time when the primary means of processing data is inoperative, compromised or otherwise unavailable. Provision should also be made for procedural deadlines to be extended to enable equal access to justice in case of system failure. To help deter unauthorised access to and processing of data held within the system, legislative measures or rules of court should make provision for such interference to be punishable by civil penalties, eg fines, astreintes or, where appropriate, imprisonment.

5. Dedicated data protection and security officers responsible for securing compliance with data protection law and the maintenance of effective data security provision within the digital justice system should be established. They should form part of the court administration and be accountable to the senior management of the court administration and the head of the judiciary. States should also establish a Digital Court Data Authority to monitor compliance with data sovereignty, protection and security requirements. This should include giving advice and guidance to those individuals who are responsible for the digitalised infrastructure. To carry this out effectively, it may liaise with a national data protection authority. The Authority should also provide an independent means through which persons may complain about the processing of their personal data by the digital civil justice system. In this respect, it may provide guidance to enable remedial action to be taken in the light of any complaint where one is upheld. To maintain judicial independence, the Authority should form part of the judiciary and be financed by dedicated funds provided to the judiciary for this purpose. It should, however, be functionally independent of the judiciary, and the court administration, in the carrying out of its responsibilities.

---

[87] As of 2025, this is ISO/IEC 27701 of 2025, which is available at: https://www.iso.org/standard/27701. Such standards are updated regularly and any updates should guide the future development of digitalisation programmes.

[88] Differential access can be secured, for instance, through requiring system users to register with the digitalised system and access it through using unique identification numbers. Registration should require provision of specified official means of identification. Care should be taken to ensure that non-nationals are able to utilise appropriate means to secure access using official means of identification available to them.

[89] A Chung & Y Yu, *Delivering Justice in the Digital Economy - Innovations in China's E- Courts*, in F de la Rosa et al (eds), *Digitalization and Artificial Intelligence in Courts: Opportunities and Challenges*, (OUP, 2025) at 178.

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9505990-6-0