"PROMOTING CYBERJUSTICE IN SPAIN THROUGH CHANGE MANAGEMENT"

SRSS/S2019/033

CO-OPERATION PROJECT
BETWEEN THE MINISTRY OF JUSTICE OF THE KINGDOM OF SPAIN AND THE EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ) FUNDED BY THE DIRECTORATE GENERAL FOR STRUCTURAL REFORM SUPPORT OF THE EUROPEAN COMMISSION

Feasibility Study for Electronic Judicial Procedure Regulations

By Giulio BORSARI, Alexandra TSVETKOVA and Elena Alina ONTANU, CEPEJ Experts

This Action was carried out with funding by the European Union via the Structural Reform Support Programme and in cooperation with the European Commission's DG Reform Support Service.
This document was produced with the financial assistance of the European Union and co-funded by the Council of Europe. The views expressed herein can in no wat be taken to reflect the official opinion of the European Union or the Council of Europe.

Table of Contents

Introduction

Within the action "Promoting Cyberjustice in Spain Through Change Management (Phase II)", Component 3 provides support to the development of electronic judicial procedure regulations in Spain. The present "Feasibility Study for Electronic Judicial Procedure Regulations" represents Output No. 3 under this component.

The topics in scope of the study have been first discussed with the representatives of the Spanish Ministry of Justice during a workshop entitled "Regulations for Electronic Judicial Procedures" that took place via videoconference on 14/4/2021 and were later detailed in the meeting report dated 22/4/2021. After further discussions with Mr. Leonid Antohi, Project Coordinator of the CEPEJ Cooperation Unit, the topics, namely regarding the right to digital disconnection, open data, automatization of decisions using AI, online alternative dispute resolution, and remote hearings (telematic trials), were finally confirmed and particular tasks assigned.[1] These five topics are explicitly discussed considering the draft Law on Digital Efficiency of the Public Service of Justice, prepared by the Spanish Ministry of Justice.

The version of the Law on Digital Efficiency of the Public Service of Justice that has been considered herein is the one received by the CEPEJ Secretariat on 28/10/2021 (in Spanish) and presented by the Spanish Ministry of Justice during a workshop entitled "Consultations on the Draft Law on Digital Efficiency Measures of the Public Service of Justice" which took place via videoconference on 25/11/2021.[2] In the present study, the respective articles of the draft law are translated in English using Google Translate or the translation tool embedded in Microsoft Word.[3]

To support this and other studies under the action, a questionnaire has been prepared by the CEPEJ Cooperation Unit and sent to 23 Member States of the Council of Europe on 7/10/2021. Two questions have been specifically prepared regarding "Right to digital disconnection" and "Remote hearings" topics discussed herein. Present report elaborates on the answers[4] provided by a total of 20 respondents; where some respondents have been directly contacted to provide further clarifications to their replies.

In the following table, main contributors per topic are indicated:

Topic	*Main contributor(s)*
1) Right to digital disconnection	Elena Alina Ontanu
2) Open data	Elena Alina Ontanu and Giulio Borsari
3) Automatization of decisions using AI	Alexandra Tsvetkova
4) Online alternative dispute resolution	Alexandra Tsvetkova
5) Remote hearings (telematic trials)	Giulio Borsari

[1] The assignments for the study were commenced to Giulio Borsari and Alexandra Tsvetkova on 9/07/2021 and to Elena Alina Ontanu on 9/11/2021.

[2] Out of the three authors of this report, only two – Elena Alina Ontanu and Giulio Borsari – were present.

[3] None of the authors of this report is a Spanish native speaker.

[4] Received by the authors via Mr. Antohi on 2/11/2021. Any further information on this survey can be provided upon request.

1 Right to Digital Disconnection

1.1 Introduction

New and emerging technologies, including devices such as laptops, tablet computers and smartphones, have revolutionized everyday work and life in the last decades enabling constant connection with work colleagues and supervisors as well as in the private sphere.[5] As teleworking or remote working practices have been gaining ground, they starting detaching work from physical spaces normally associated with professional activity and starting entering the private sphere as internet connection allows work to be carried out basically at any time and from any space. According to Messenger, "this new independence of work from place changes the role of technology in the work environment dramatically".[6] And while at first it may have concern some of the highly skilled workers having access to these technologies, now it can be linked to new rising forms of work such as work-on-demand-via-app or crowdsourcing. These new forms increase further the possibilities of remote working and extend it to other domains such as manufacturing, physical services with a relevant effect on a tendency of reducing resting time and pauses on connection with what could be seen as an increased flexibility of workers.[7] The changes have been accelerated since March 2020 when home working became a necessity in many countries. To contain the spread of the COVID-19 pandemic, many Europeans stopped going to the office and shifted to working from home at the request of their governments and employers. As a result, teleworking or remote working grew exponentially within the EU.

The interest to adopt dedicated rules in relation to a right to disconnect from technology devices when carrying out teleworking or remote working has begun to be considered in some countries to allow staff and management to ignore work related matters outside the formal working hours, except for exceptional or force majeure circumstances. Such considerations were made as early as the beginning of the 2000s in France and Germany for example. Nevertheless, dedicated rules or legislative projects started to be tabled almost two decades later. This trend has been gaining ground with the increase of teleworking and remote working needs due to COVID-19 pandemic. Having specific rules was perceived as a need to accommodate this switch to mobile and flexible time and space way of working within the existing labour legislation, creating a legal framework to maintain a balance between work and private life spheres. Furthermore, this legislative impulse has not been related only to labour legislation and collective labour agreements but has been connected also to other areas of law such as matters of privacy of data or have been considered in legislative proposals related to digitalisation of the judiciary (e.g., Spain).

[5] Jon C. Messenger, *Working Anytime, Anywhere: the Evolution of Teleworking and its Effects on the World of Work*, IUSLabor (2017)3, p. 303.

[6] Ibid, p. 303.

[7] Matte Avogaro, *"Right to disconnect: French and Italian Proposals for a Global Issue"*, *RDRST*, Brasilia, 4(2018)3, p. 110.

1.2 Defining the Right to Disconnect

In literature, available case law, dedicated national legislation and private business initiatives (e.g., collective agreements concluded at company level) the right to disconnect is addressed in relation to labour relations in seeking to attain and guarantee a better work-life balance. According to European Foundation for the Improvement of Living and Working Conditions (Eurofound) the right to disconnect should be understood as the workers' right to be able to disengage from work and refrain from engaging in work-related electronic communications (e.g., emails, text messages, chat, other type of messages, phone calls, online meetings) outside the working hours, during holidays,[8] maternity and paternity leave, and other forms of leave.

The development and widespread use of smart phones, other digital devices and communication applications has resulted in employees always being "on call" in many workplaces and a pressure on these to be constantly available or accessible for mobile or online communications.[9] It is also becoming usual for contracts to include a duty for employees to be available after working hours,[10] during weekends and holidays. As such being prompt is associated with high productivity and a condition for career advancement.[11] For this reason, employees find themselves under significant constrain to consent to such practices and continue working after working hours.

Studies carried out in several countries for Eurofound revealed that teleworkers and workers carrying out their work via information and communication technology are in general more likely to perform paid work in the evenings and on weekends than those workers who always work in the office and at the same time enjoy a significant degree of working time autonomy compared to their office-based counterparts. This is important in relation to the reported work–life balance of workers. The findings seem to be related also to country-specific working time patterns, cultures, and gender roles.[12]

A widespread increase in online working is seen as having positive as well as negative effects on work-life balance the outcome of studies are mixed. On one hand, this way of working, particularly when working from home, appears to have a positive effect on overall work-life balance because of the reduction in commuting time and increased autonomy to organize working time based on individual workers' needs and preferences. On the other hand, there is some risk of overlap between work and private life because of longer hours of home-work and the combination of paid work and other responsibilities increasing the chances of work-family conflict. Such arrangements can easily lead to working beyond the amount of normal contractual working hours and this often appears to remain

[8] Eurofound, EurWORK, *The Right to Disconnect*, 22 October 2019.

[9] Klaus Müller, *The Right to Disconnect*, Briefing, European Parliamentary Research Service, PE 642.847, July 2020, p. 1.

[10] "After working hours" can have a broad definition as this can differ in various jurisdictions and depends on when an employer expects an employee to be available, but does not necessarily refer to any specific time period. It can be for example from 9 am to 5 pm or from 9 pm to 5 am. Thus, is should be understood as any time an employee is off duty.

[11] Op. cit. *The Right to Disconnect*, Briefing, p. 1, referring to IW Köln, *Zur Ambivalenz flexiblen Arbeitens. Der Einfluss betrieblicher Familienfreundlichkeit*, 2019.

[12] Op. cit., *Working Anytime, Anywhere: the Evolution of Teleworking and its Effects on the World of Work*, p. 305.

unpaid. [13] This is confirmed also by the findings of Vargas Llave, Tina Weber and Matteo Avogaro who conclude that telework affords an increased productivity, a better work-life balance and greater working-time autonomy, but at the same time it can result in a blur of boundaries between people's professional and private lives.[14]Furthermore, the expectation that workers are available at almost any time is considered to be potentially hazardous to workers' health,[15] privacy and private life especially as online working is expected to "become increasingly common" in the future.[16] This is of significant importance as the developments of remote working during the COVID-19 crisis has led to an increase of online working and employees being connected via various applications. Additionally, even greater concern is the fact that "the monitoring of employee mobile devices can often allow employers to obtain GPS tracking information through which employers can uncover employees' locations, daily routines, private sexual information, and medical conditions".[17]

1.3 Existing National Regulations in the European Union

While there is currently no dedicated European framework expressly defining and regulating the right to disconnect, a legislative proposal has been initiated and is addressed hereafter. At present primary and secondary EU legislation address several aspects related to working conditions, social security and social protection of workers that can be indirectly related to the right to disconnect.

1.3.1 Primary EU Law Provisions

Several provisions in the Treaty on the Functioning of the European Union (TFEU) and Article 31 of Charter of Fundamental Rights of the EU (Charter) are of relevance in relation to this topic.

Art 153 and Art 154 TFEU establish a duty on the EU to support and complement the Member States' activities and adopt directives concerning the minimum requirements for working conditions in the EU. According to Art 153(2) TFEU, such legislation must also address aspects of social security and social protection of workers. Social partners are to be consulted on possible initiatives envisaged under Art 153 TFEU (Art 154TFEU), and they can sign agreements, which, upon their request, can be implemented at EU level in accordance with Art 155 TFEU. Further social partners may also collect and exchange good practices across the EU in this area, while at national level social partners can support the implementation of such legislation or good practices via collective bargaining and through involvement in the design and implementation of relevant policies. Additionally, Art 31 Charter on Fundamental Rights of the European Union on "Fair and just working conditions" gives every worker the right to

[13] Ibid, p. 306.

[14] Background summary report for a webinar on the right to disconnect, Oscar Vargas Llave, Tina Weber, Matteo Avogaro, Eurofound, June 2020.

[15] See example of Japanese worker – *karoshi* – killed herself of too much working due to heart failure. Justin McCurry, *"Japanese Woman Dies from Overwork' After Logging 159 Hours of Overtime in a Month"*, *The Guardian*, 5 October 2017.

[16] Op. cit. *The Right to Disconnect*, Briefing, p. 1; Eurostat, *How usual is it to work from home?*, April 2019.

[17] Paul M. Secunda, *"The Employee Right to Disconnect"*, Notre Dame Journal of International & Comparative Law, 9(2019), Article 3.

working condition that respect his or her health, safety, and dignity. Thus, indirectly the text addresses aspects that are to be protected across a right to disconnect.

1.3.2 Secondary EU Legislation

The present EU legislation regulates a number of rights that indirectly refer to similar issues that would be addressed by the right to digitally disconnect although they do not identify it as such. Also, the various adopted directives do not specifically address workers' rights to disconnect from digital tools including information and communication technology. Available legislation includes:

- The Working Time Directive (2003/88)[18] provides a legal framework that sets a maximum working week of 48 hours, including overtime (Art 6). The reference period should not exceed four months but may be extended to a maximum of six months, and, under certain conditions (e.g., in the case of a collective agreement), it may be extended to a maximum of one year. This is an important provision because studies point towards teleworkers or online employees being more likely to report long weekly working hours than other workers. In addition, the directive contains provisions on the minimum daily rest of eleven consecutive hours (Art 3), rest breaks for working day longer than six hours (Art 4) and weekly minimum rest period of twenty-four hours (Art 6),[19] and an annual leave of at least four weeks (Art 7(1)) for preserving the worker's health and safety. The Court of Justice of the European Union (CJEU) has emphasised that these minimum requirements "constitute rules of Community social law of particular importance from which every worker must benefit as a minimum requirement necessary to ensure protection of his safety and health".[20]
- Directive (EU) 2019/1152 on transparent and predictable working conditions in the European Union[21] establishes that provisions on the place of work and work patterns have to be included in employee contracts. This makes the working conditions for teleworkers and workers working via information and communication technology means more transparent and predictable from the outset of the employment relationship. Moreover, the directive seeks to protect workers from on-demand requests by specifying that they have to be given a reasonable period of advanced notice about when work will take place (Art 10). This could help to reduce the unpredictability of irregular working time patterns and have a positive impact on the work-life balance of workers.

[18] Directive (EC) No 2003/88 concerning certain aspects of the organization of working time, OJ L 299/2003 p 9.

[19] This can be averaged for a period of two weeks.

[20] CJEU, Judgment of 7 September 2006, *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland*, C-484/04, ECLI:EU:C:2006:526, para 38; CJEU, Judgment of 14 October 2010, *Union syndicale Solidaires Isère v Premier ministre and Others*, C-428/09, ECLI:EU:C:2010:612, para 36.

[21] Directive (EU) 2019/1152 on transparent and predictable working conditions in the European Union OJ L 186/2019, p. 105.

- Directive on Work-Life Balance for Parents and Carers (2019/1158)[22] extends the existing right to request flexible working arrangements to all working parents of children up to eight years old and all carers. This should be facilitated, where possible, through remote working arrangements, flexible working schedules or a reduction in working hours.

Together with this, two soft law instruments are available:

- Principles 9 (Work-Life Balance) and 10 (Healthy, Safe and Well-adapted Work Environment and Data Protection) of the European Pillar of Social Rights,[23] and
- European Framework Agreement on Telework, signed by the social partners in 2002; the agreement is implemented simply as a set of guidelines for good practice.[24]

Lastly, the Working Time Directive defines the working time in Art 2(1) as "any period during which the worker is working,[25] at the employer's disposal and carrying out his activities or duties, in accordance with national laws and/or practice".[26] The case law of the Court of Justice of the European Union linked to the Working Time Directive also distinguishes between "on-call time" and "stand-by time". "On-call time" is performed at the employer's premises and is counted as working time even if it is "inactive". "Stand-by time" is where a worker is at home or a place of their choosing but required to be contactable and ready to work if called upon.[27] The working time is counted only for the hours actually worked.[28] Additionally, the working time has to be documented; therefore a system measuring the duration of time worked each day by each worker has to be set up.[29]

1.3.3 Legislative Proposal

The research carried out by Eurofound showed that people who work regularly from home are more than twice likely to surpass the maximum 48 hours of work per week, compared to employees working from their employer's premises. Also, almost 30% of those working from home reported working in their free time every day or several times a week to meet work demands compared to 5% if those working from their employer's premises. The increased use of digital tools for work purposes has resulted thus in an "everconnected", "always on", or "constantly on-call" culture. According to the European Parliament, this can have detrimental effect on workers' fundamental rights and fair working

[22] Council Directive 2019/1158 on work-life balance for parents and carers and repealing Council Directive 2010/18/EU, OJ L 188/2019, p. 79.

[23] The European Pillar of Social Rights in 20 Principles.

[24] As soft law instruments could easily be circumvented. That is why we need mandatory regulation at European level on all issues of telework.

[25] "At work" in some language versions such as French, Italian, Spanish, and Romanian.

[26] See Report on the implementation by Member States of Directive 2003/88/EC concerning certain aspects of the organisation of working time, SWD(2017) 0204 final, European Commission, April 2017.

[27] CJEU, Judgment of 21 February 2018, *Ville de Nivelles v Rudy Matzak*, Case C-518/15: stand-by time of a worker at home who is obliged to respond to calls from the employer within a short period must be regarded as "working time"; CJEU, Judgment of 14 May 2019, *Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SA*, Case-C-55/18.

[28] CJEU, Judgment of 21 February 2018, *Ville de Nivelles v Rudy Matzak*, Case C-518/15

[29] CJEU, Judgment of 14 May 2019, *Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SA*, Case-C-55/18.

conditions, including fair remuneration for the time worked, "the limitation of working time and work-life balance, physical and mental health and safety at work and well-being" and result in a disproportionate impact on workers with caring responsibilities who are often women.[30] Additionally, "excessive use of technological devices can aggravate phenomena such as isolation, techno-addiction, sleep deprivation, emotional exhaustion, anxiety and burnout".[31]The COVID-19 crisis lead to more working from home where long working hours and higher demands only further enhanced these negative effects, while at the same time underlining the importance of digital solutions and the alternative they provide for companies and public administration to continue to offer their services during crisis periods.

Based on available data, the European Parliament decided to call on the European Commission to make a legislative proposal that enables those who work digitally to disconnect outside their working hours. The members of the European Parliament ("MEPs") consider the right to disconnect to be a "fundamental right that allows workers to refrain from engaging in work-related tasks" (e.g. work related phone calls, emails, other digital communications) outside the working hours, during holidays or other forms of leave.[32] This should be seen as "an inseparable part of the new working patterns in the new digital era; whereas that right should be seen as an important social policy instrument at Union level to ensure protection of the rights of all workers" and having a particular strong importance for "vulnerable workers" and workers "caring responsibilities" according to the European Parliament resolution.[33] This legislation proposal was set to establish minimum requirements for remote working and clarify working conditions (including the provision, use and liability of equipment, such as of existing and new digital tools), working hours and rest periods,[34] and ensure that such work is carried out on a voluntary basis and that the rights, workload and performance standards of digital remote workers are equivalent to comparable on premises workers. This aims to address the "always on" culture created by the increase in digital resources used for work purposes which lead to negative effects in employees such as anxiety, depression, burnout, other mental and physical health issues.

According to the European Parliament resolution a directive proposal on the right to disconnect should "particularise, complement and fully respect the requirements laid down in Directive 2003/88/EC concerning certain aspects of the organisation of working time, in particular as regards the right to paid annual leave, in Directive (EU) 2019/1152 on transparent and predictable working conditions, in Directive (EU) 2019/1158 on work-life balance for parents and carers and in Council Directive 89/391/EEC on the safety and health of workers, and in particular the requirements in those directives that relate to maximum working hours and minimum rest periods, flexible working arrangements, and information obligations, and should not have any negative effect on workers; believes that the new directive should provide for solutions to address existing models, the role of the social partners, the

[30] European Parliament Resolution of 21 January 2021.

[31] Ibid.

[32] European Parliament, *"Right to disconnect' should be an EU-wide fundamental right, MEPs say"*, Press Releases, 21.01.2021.

[33] Op. cit. European Parliament Resolution of 21 January 2021.

[34] Op. cit. *"Right to disconnect' should be an EU-wide fundamental right, MEPs say"*.

responsibilities of employers and the needs of workers regarding the organisation of their working time when they use digital tools; highlights the fundamental importance of the correct transposition, implementation and application of Union rules and recalls that the employment and social acquis of the Union fully applies to the digital transition; calls on the Commission and the Member States to ensure proper enforcement through the national labour inspection authorities".[35]

The proposal emphasises the fact that employers should not require their employees to be directly or indirectly available or reachable outside their working time and co-workers should refrain from contacting their colleagues for work purposes outside the agreed working time.[36]

The legislative proposal is set to be based on Art 153(1)(a)-(b) and (i) TFEU setting a duty on the EU to support and complement the activities of the Member States to improve the working environment to protect workers' health and safety, working conditions and of equality between men and women with regard to labour market opportunities and treatment at work, and Art 31 Charter. The proposal aims to improve working conditions for all workers by laying down minimum requirements for the right to disconnect (Recital 20 of the proposed directive) and concerns private employers as well as public administration (Art 1(1) Directive Proposal). The recommendation of the European Parliament to the European Commission is for the proposal to follow a minimum level of harmonisation approach across Member States that does not prevent them to adopt provisions which offer a higher level of protection to workers (Art 9(2) Directive Proposal).

The text of the proposed directive contains provisions on EU Member States duty to take measures to ensure:

- employers provide workers with means to exercise right to disconnect (Art 3(1))
- employers set up an objective, reliable and accessible system enabling the duration of time worked each day by each worker to be measured, in accordance with workers' right to privacy and to the protection of their personal data (Art 3(2))
- measures to implement the right to disconnect in consultation with social partners (e.g., arrangements for switching off digital tools including work-related monitoring tools, system for measuring working time, health and safety assessment, criteria for derogation to implement worker's right to disconnect, compensation for work performed outside working hours, training and awareness-raising measures) (Art 4(1))
- possibility to conclude collective agreements at national, regional, sectorial or employer level (Art 4(2))
- protection against adverse treatment for exercising right to disconnect (Art 5)
- right to redress in case of violation of right to disconnect (Art 6)

[35] Op. cit. European Parliament Resolution of 21 January 2021.

[36] Ibid.

- employers' obligation to provide each worker in writing with clear, sufficient and adequate information on their right to disconnect, including a statement setting out the terms of any applicable collective or other agreements (Art 7)
- lay down rules on penalties for infringements of national provisions regarding right to disconnect (Art 8).

1.4 Data Protection Aspects

An aspect that needs to be considered in relation to the right to disconnect but is not going to be further elaborated on for the purpose of this report, is related to data protection. This is due to the fact technology advancements are adding a new layer of complexity to monitoring and surveillance of work carried out via information and communication technology. While the use of intrusive digital technologies in the workplace is to some extent addressed and regulated in some Member States, surveillance of teleworking is not.

Art 8 of the European Convention of Human Rights (ECHR) provides that "everyone has the right to the protection of personal data concerning him or her". This right has been used at national level in several countries to protect employees' privacy in the employment context, therefore, this is of relevance also for practices of protection of personal data when work is carried out remotely or the employee is engaged in teleworking.

In addition to Art 8 ECHR, the General Data Protection Regulation (GDPR) provisions[37] are set to guarantee that employees receive adequate information on the scope and nature of the monitoring and surveillance and that employers are required to justify the measures and minimise their impact by deploying the least intrusive methods.[38] The use of technology should not result in concerns as regard to the privacy of the employees self-determination in their work or disproportionate and illegal collection of personal data, surveillance and monitoring of workers.

1.5 National Approaches of EU Member States

The approach of EU Member States towards the regulation of the "right to disconnect" is fragmented and not all countries included it in their legislation. In recent years more extensive actions to regulate online work – teleworking or remote working – and the use of digital communication means have been taken to provide protection to employees in some Member States. For example, legislation has been adopted in Belgium, France, Italy, Spain, while proposals have been tabled in the Netherlands and Portugal (a proposal was rejected in Portugal in 2019). In most cases where it is regulated the details related to its application and effective implementation is to be carried out at sectoral or company level via collective agreements. Thus, the legislation where available requires the social partners at sectoral or company level, or the individual employee, to reach an agreement on how to make this right

[37] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

[38] Op. cit. European Parliament Resolution of 21 January 2021.

operational. These developments have been brought about in the context of an increasingly digitalized and flexible work. As an overall approach of the new national legislation, it is important to underline that the rules are often based on pre-existing national social partner agreements (e.g., France) or on company practices (e.g., Italy).[39]

Research carried out by Eurofound classified[40] these initiatives as:

- "**balanced promote-protect**" approach: where specific legislation introducing a legal framework for the right to disconnect was established (e.g., Belgium, France, Italy, and Spain)
- "**promoting**" approach: legislation on the use of telework, with provisions identifying its potential advantages but not its potential disadvantages (e.g., Czechia, Lithuania, Poland, and Portugal)
- "**general"** regulatory approach: only general legislation regulating the use of tele/remote work (e.g., Austria, Bulgaria, Estonia, Germany, Greece, Croatia, Hungary, Luxembourg, Malta, the Netherlands,[41] Romania, Slovenia, and Slovakia)
- **no specific legislation** governing tele- or remote working (e.g., Cyprus, Denmark, Finland, Ireland, Latvia, and Sweden).

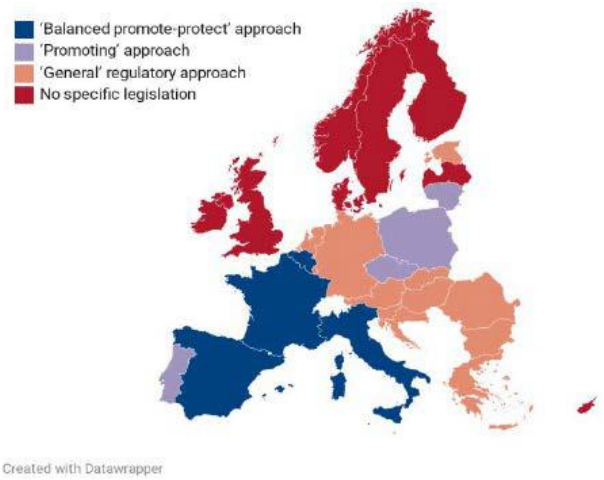

Figure 1. Cluster analysis of national legislation (2020) in European Parliament Briefing[42]

While there is legislation in some countries, the right to disconnect is not universally accepted as a necessary right because the Working Time Directive already provides for maximum working hours.

[39] Eurofound (2020), *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, Publications Office of the European Union, Luxembourg, p. 51.

[40] Op. cit. Background summary report for a webinar on the right to disconnect, Eurofound, June 2020.

[41] The Netherlands is expected to move in the future to the "balanced promote-protect" approach based on a legislative project tabled with the Dutch legislation in relation to the right to disconnect.

[42] Op. cit. *The Right to Disconnect*, Briefing, p. 3.

Several national court cases have ruled on this issue (e.g., the Kepak case in Ireland)[43] and the CJEU established that the employers must establish systems to record working hours (i.e., C-55/18 CCOO).[44] Other countries have chosen to rely on collective bargaining and company practice to regulate teleworking or remote working in order to secure a work–life balance and the right to disconnect. However, such approaches can lead to inequalities between countries and sectors as well as between types of workers who may not have strong representation in collective bargaining at different levels.[45]

1.5.1 Information from Other Countries

On the topic of right to disconnect of persons engaged in judicial procedures, the survey carried out by Secretariat of the European Commission for the Efficiency of Justice to the Council of Europe (CEPEJ) among some of the Council of Europe member States sought to establish whether there is national legislation in place or under discussion in relation to the justice sector and whether this concerns the users of the justice services or the professional actors.

Possible answers were:

1. No, because there are no provisions on digital communication in judicial proceedings, therefore there is no need for regulation of the right to digital disconnection.
2. No. Although there is regulation on digital communication in judicial proceedings, there is no specific regulation of the right to digital disconnection.
3. Yes, the right to digital disconnection is regulated regarding lay citizens as court users.
4. Yes, the right to digital disconnection is regulated regarding professional court users (judges, lawyers, prosecutors, court staff etc.).
5. There is no regulation, but there is a relevant study or draft legislation.
6. Other.

The following table summarises the answers provided:

[43] Kepak Convenience Foods Unlimited Company v Grainne O'Hara (DWT1820) highlighted the issue of weekly working limits and the increased use of emails outside working hours. The core of the case was the issue of the employee having received and replied to emails between 5pm and midnight on a number of occasions – hours which fall outside her normal working hours. This case highlights the importance of the employer maintaining good records of working hours, but also of the need to keep an awareness of work being done outside office hours. It has been suggested that smartphones cause employees to work longer through being contactable on emails. Employers should be mindful of this to ensure employees are not working beyond the statutory limit on a regular basis to avoid claims being brought.

[44] CJEU, C-55/18, *Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE*, ECLI:EU:C:2019:402.

[45] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 51.

Country	1	2	3	4	5	6	Comments
Cyprus		x					-
Austria						x	The idea of digital disconnection is not a current topic in AT. While the internal justice system will work completely digital, parties will still get analogue and digital channels to participate in proceedings.
Ireland		x					-
Switzerland			x				Currently there is no obligation to communicate electronically with the judicial authorities. A law in preparation foresees to oblige only the professional representatives of the parties (lawyers)
North Macedonia	x						-
Slovakia (Ministry of Justice)	x						The general answer is NO. There are specific agendas, where electronic communication is mandatory, but there is no "justice specific" regulation of the right to digital disconnection
Slovakia				x			This is regulated in the court's work schedule.
Luxembourg	x						-
Germany		x					Means of digital communication in judicial proceedings are always provided as additional ways to access the justice system and do not replace the conventional means.
Monaco		x					-
Bosnia & Herzegovina		x					-
Sweden	x						-
Norway		x					-
Latvia						x	In various procedural laws it is regulated when the court hearing can be suspended (mostly due to the illness) for both - citizens and professional practitioners and the Court decide when it will be applicable. However, at the moment it is not regulated when persons can use right to disconnect in remote hearing/videoconference aspect.
The Netherlands				x			The person who leads the interrogation or the court decides whether or not videoconferencing will be used after discussing this with the parties concerned. This and other principles have been laid down in national legislation: https://wetten.overheid.nl/BWBR0019836/2020-03-25
Lithuania		x					-
Ukraine		x					-
Slovenia		x					Rules on electronic operations in civil procedures and in criminal procedure, http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV13993
France		x					-

In analysing the responses received to the survey and comparing them with the developments related to the regulation of the right to disconnect in the jurisdictions that were further investigated (in particular, France and the Netherlands) a certain discrepancy is revealed.

The reasons for this difference of perception are not clear but they are potentially due to a misunderstanding or interpretation of the question from the perspective of other questions included in the survey such as the ones dedicated to videoconferencing for remote hearings (i.e., the Netherlands). As a result, the outcome of the survey could not be used to supplement the desk research on the right to disconnect. Lastly, it has to be underlined that the right to disconnect is generally addressed in the jurisdictions further analysed from a labour law perspective and not particularly from that of judicial authorities or procedural law perspectives.[46]

1.5.2 France

France is an EU pioneer in addressing the right to disconnect (*droit à la déconnexion*).[47] In 2013 a national cross-sectoral agreement on quality of life at work was set to encourage businesses not to intrude on employees' private lives by defining periods when their electronic devices could remain switched off.

A legislative proposal followed in 2016 and led to the adoption of paragraph 7 of Art L2242-8 Labour Code which became applicable on 1 January 2017. The provision covers workers subject to *forfait en heures* or *forfait en jours* regime for companies having at least fifty employees.[48] Given this provision of the French Labour Code, France has been included by Eurofound in the category of countries having "very high coverage – right to disconnect".[49] Further, the article now L2242-17(7) Labour Code was modified in 2019[50] to the present text that states:

> *The annual negotiations on equal opportunities between women and men and the quality of working life cover:*
>
> *(7) The terms enabling employees to fully exercise their right to disconnect and the introduction by the company of schemes regulating the use of digital devices, with a view to ensuring compliance with regulations governing rest and leave periods, privacy and family life. In case an agreement cannot be reached between the employer and the employees, the employer will adopt a charter after obtaining an opinion of the economic and social committee. The charter will address the ways in which the right to disconnect will be exercised as well as the*

[46] Some exception appears to be the current draft on of Law on digital efficiency in Spain and the Italian legislation that addresses more generally the public administration. See further sub-sections 1.5.4 and sub-section 1.6.

[47] Op. cit. *"The Employee Right to Disconnect"*, p. 27.

[48] Loi Travail du 8 août 2016.

[49] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 51.

[50] Article L2242-17 was modified by LOI n°2019-1428 du 24 décembre 2019 - art. 82 (V).

> *implementation for the employees and the administration of actions to train and raise awareness with regard to a reasonable use of electronic devices*.[51]

The provision is a general one that delegates the details of this right to social partners via collective agreements which are set to establish both mandatory provisions and sanctions in case of illegal conduct, and programmatic declarations aimed to introduce policies directed to maintaining work-life balance and address the risks related to remote work. Thus, in France the right to disconnect has to be included in the mandatory annual negotiation process focussing on quality of life at work and gender equality. This has a broad application as it concerns all companies subject to mandatory collective agreements and not only workers that have a contract including flexible working arrangements via a *forfait-jours* (fixed annual number of working days) clause.

The collective agreements once adopted are part of the internal company regulation and subject to provisions of French law imposing the involvement of trade unions. The limitations of L2242-17(7) Labour Code are that it is applicable only to employers with fifty or more employees, but as these legislative provisions are supplemented with collective agreements in almost all sectors, this covers more companies.[52] Companies are expected to include this matter in the negotiations with the employees' representatives, but they are not required to actually sign a collective agreement on the right to disconnect. The law does not sanction them if no agreement is reached. However, if the company disregards the obligation to negotiate, this can result in criminal liability, with a maximum one-year prison term and a fine up to 3,750 Euros for the company's legal representative and a fine up to 18,750 Euros for the company based on Art L2243-2 of the French Labour Code. These legal provisions are further supplemented by universally applicable sectoral collective agreements, as well as by company-level agreements. Therefore, this can increase the level of coverage and extend it to the majority of the workforce. The conclusion of such agreements that contain specific provisions on the right to disconnect grew following the adoption of Art L2242-17 Labour Code,[53] but such agreements existed also beforehand. For example, even prior to the coming into application of the Art L2242-17, on 27 September 2016, some French companies had included specific provisions in their company's collective agreements. This was as early as 2012 for Axa or Areva which granted a right to disconnect in their respective collective agreements. Syntec's collective agreement included the right to disconnect

[51] Article L2242-17 Labour Code:

> *"La négociation annuelle sur l'égalité professionnelle entre les femmes et les hommes et la qualité de vie au travail porte sur:*
>
> *1° L'articulation entre la vie personnelle et la vie professionnelle pour les salariés;*
>
> *(…)*
>
> *7° Les modalités du plein exercice par le salarié de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale. A défaut d'accord, l'employeur élabore une charte, après avis du comité social et économique. Cette charte définit ces modalités de l'exercice du droit à la déconnexion et prévoit en outre la mise en œuvre, à destination des salariés et du personnel d'encadrement et de direction, d'actions de formation et de sensibilisation à un usage raisonnable des outils numériques."*

[52] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 51.

[53] Eurofound (2021), *Working Conditions. Right to Disconnect: Exploring Company Practices*, Publications Office of the European Union, Luxembourg, p. 19.

in its April 2014 amendment to their working time agreement, with "an obligation to disconnect distant communication tools". As a result, all companies within the scope of this collective agreement had to implement such obligation. The Wholesale Trade (*Commerce de Gros*) collective agreement from 30 June 2016 also inserted such obligation in its addendum on working time. The telecommunications group Orange France collective agreement was also mindful of the digital transformation and established a right for its employees to disconnect. Bruno Mettling, HR Director at Orange published a report in 2015 on digital transformation and quality of life at work. He considered that disconnecting from work was both a right and a duty (*un droit et un devoir*). His report became a source of inspiration and a starting point for the 2016 Labour Code provision. Other similar examples were adopted in the investment banking and financial services by Natixis and Société Générale.[54] Such rules can concern both the employees and to employers, namely: having a duty for employees to leave in the office at the end of their working days the electronic devices of the company or the employer may have a policy or duty of switching off the servers at the end of the working day or for internal e-mails or messages sent outside the ordinary working time, alternatively a disclaimer would be displayed indicating that an immediate reply is not requested or opting to use indicators showing how urgent a reply is in internal communication.[55]

Alternatively, if no agreement is reached between employers and trade unions, this leads to the duty to adopt of charters of good conduct that establish when employees should and should not respond to electronic communication after working hours.[56] In drafting the charter the employers are required to have a prior consultation with their social and economic committee. The charter has to establish the procedures for exercising the right to disconnect and should include provisions regarding training and awareness raising for employees, managers and executives in relation to this right. The downside of relying on a charter or company-level agreement is that they are non-binding, and no sanctions are imposed as such for breaching them.

Further, electronic requests made beyond working hours are to be seen as compensable time, just "as if someone was having work phone conversations outside of normal business hours or reviewing files".[57]

Regarding court practices, the right to disconnect was recognized by French Courts prior to the adoption of Art L2242-17(2) Labour Code. On a more general approach the intrusive nature of work in employee's personal life has already been sanctioned as early as 2001. The French Court of Cassation (*Cour de Cassation*) ruled in October 2001 that an employee "is under no obligation to accept taking work back home, nor to set up work instruments and file processing at home".[58] This was followed in 2004 by a ruling by the same court that "not being reachable outside of working hours on a personal cell phone

[54] Op. cit., Eurofound, EurWORK, *Right to disconnect*, 22 October 2019.

[55] See further Henri Guyot, "L'adaptation du droit du travail à l'ére numérique », *La Semaine Juridique Social*, (2016)37, 20, p. 1310.

[56] Op. cit. *"The Employee Right to Disconnect"*, p. 28.

[57] Donalee Moulton, The Problem With a 'Right to Disconnect' Law, L. DAILY (CAN.) 11 April 2017, quoting Canadian attorney Katherine Poirier.

[58] Cass. Soc. 2 October 2001, n° 99-42727.

is not of wrongful nature and cannot be used to justify dismissal on disciplinary grounds based on serious and negligent breach of duty by the employee".[59] Further, in 2017 the Court of Cassation ordered Rentokil Initial, a British pest-control and hygiene company, to pay €60,868.51 to one of its former France-based employees agency director for having required him to be constantly accessible by telephone (on standby) in case a work issue arose from his subordinates or clients, including outside the working hours and days.[60]

Following the entrance into application of Art L2242-17(7) Labour Code not much information is available on the application and enforcement of its provisions by French authorities. For example, besides the usual general channels available to bring complaints in court, no dedicated administrative mechanism to bring claims in relation to the right to disconnect. Furthermore, there is also no general audit mechanism for authorities to verify employers' compliance with the provisions of Art L2242-17(7) Labour Code.

1.5.3 Belgium

Belgium as France is considered a "very high coverage – right to disconnect" country. The Law on Strengthening Economic Growth and Social Cohesion (*Loi relative au renforcement de la croissanec économique et de la cohésion sociale*) was adopted on 26 March 2018 and includes a section dedicated to disconnection and use of digital communication needs (Section 2, Chapter 2 – *Concertation sur la deconnexion et l'utilisation des moyens de communication digitaux*).[61] Thus, the employees have a right to discuss issues of disconnection with their employers, but "they do not have a right to disconnect in the strict sense of the term".[62]The objective of the provision is to guarantee observance of the employees' rest periods, holidays, and leave, and secure a balance between work and private life time.[63]As in France the provisions apply to companies having more than 50 employees and make it mandatory to discuss the issue of disconnection and the use of digital tools.

Art 16 of the Law on Strengthening Economic Growth and Social Cohesion requires employers to consult and negotiate with their Committee for the Prevention and Safety at Workplace (*Comité pour la Prévention et la Protection au Travail*)[64] about the use of digital communication tools and disconnection from work at regular intervals. The law does not specify how often the employer should meet with the committee but mentions that this should take place regularly and whenever the employee

[59] Cass. Soc. 17 février 2004, n° 01-45889.

[60] Cass, Soc, 12 juillet 2017 n° 17-13.029.

[61] Available at https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018032601&table_name=loi. The law was criticized by trade union representatives because it establishes "a flexibility tailored to employers", without helping to achieve a proper balance of private and professional life, guaranteeing the well-being of workers and responding to the new realities of work and business needs (Fédération Générale du Travail de Belgique, 2017).

[62] UNI Global Union, Legislating the Right to Disconnect (October, 2020), p. 6.

[63] Ibid, p. 5.

[64] Having such a committee this is a legal requirement in companies with more than fifty employees.

representatives request it. If there is no such committee in place, the trade union delegation can play this role instead in Belgium.[65]

These provisions are supplemented by collective labour agreements in various sectors which also include provisions in relation to a right to disconnect. The universally applicable national collective agreements help to promote telework and limit the working hours for this type of working arrangements. Sectoral agreements tend to reiterate the requirements set out in legislation and national collective agreements. The company-level agreements add to the above agreements and represent the main level for determining the details of teleworking and the right to disconnect for individual employees.[66] For example, at Solvay the right to disconnect was first discussed already in 2016 (two years prior to the adoption of the Belgian legislation containing provisions on the right to disconnect),[67] other company agreements containing such provisions are at KBC, De Lijn, and Lidl, and were adopted in 2018.[68] Overall, a number of universally applicable sectoral collective agreements and company agreements addressing the right to disconnect are in place and they are estimated to extend the coverage of the provisions regarding disconnection to beyond the 47% of workers employed in companies with more than 50 employees.[69] However, if a company's Committee for the Prevention and Safety at Workplace and the management fail to reach agreement on the issue, the company is not obliged to issue a charter on the right to disconnect, as is the case in France.[70]

1.5.4 Italy

In 2016 the Government as well as a group of parliamentarians made two proposals to regulate the right to disconnect. This was framed within a more general legislation dedicated to smart working (*lavoro agile*).[71] The initiative was partly inspired by the French developments.

The text related to a right to disconnect was adopted in 2017. This is contained in Art 18 of Law No 81 of 22 May 2017 – known as the *Lavoro Agile* Law:

[65] Op. cit. UNI Global Union, *Legislating the Right to Disconnect* (October, 2020), p. 6.

[66] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 47.

[67] Between 20% and 25% of Solvay's managerial staff in Belgium teleworked at least one or two days per week. See indication in op. cit. *Working Conditions. Right to Disconnect: Exploring Company Practices*, p. 24

[68] Op. cit. *Working Conditions. Right to Disconnect: Exploring Company Practices*, p. 24.

[69] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 51.

[70] Op. cit. *Working Conditions. Right to Disconnect: Exploring Company Practices*, p. 18.

[71] Bills No. 2229 and 2233 introduced in the Italian Senate. Bill No. 2229, proposed by the members of the Parliament explicitly recognized the right to disconnect in Art 3(7) of the proposal which indicated that the workers "have right to disconnect from technological devices and from on-line platforms without bearing any consequence on the prosecution of the labour relationship and on compensation". Bill No. 22339 introduced by the Government proposed in Art 16 the introduction of the right to disconnect provision. The text proposed the adoption of a form of mandatory agreement between a worker and an employer to access and regulate the smart working regime. In their agreement the parties had a duty to indicate the technical and organisational measures that would functionally secure for the employee the right to disconnect from technological devices utilized to realize the performance. In the legislative process the Bills No. 2229 and No. 2233 of 2016 were then joined in a common proposal – Bill No. 2233-B – adopted by the Parliament as part of Law No. 81/201740.

> "1. *The provisions of this chapter, in order to increase the competitiveness and facilitate the reconciliation of private life times and work, promote agile work as a way of executing the employment relationship established by agreement between the parties, even with forms of organization by phases, cycles and objectives and without precise constraints of time or place of work, with the possible use of technological tools for the performance of the work activity. The work performance is performed, partly inside company premises and partly outside without a fixed location, within the limits of maximum duration only of daily and weekly working hours, deriving from the law and collective agreement*."

With this law the Italian legislator has established a specific method of carrying out subordinate work remotely, giving it autonomous regulation and differentiating it from remote work as new form of carrying out teleworking. It concerns both the public[72] and private sector.[73]

As a general consideration the Italian legislative provisions are unique in the sense that they have opted to assign the responsibility for reaching an agreement to individual employers and employees (rather than representatives of employees or trade unions). This arguably implies a different power balance between the parties.[74] The right to disconnect is a mandatory element of the individual agreement and only applies in the case of so called "smart workers" specific contractual status. Therefore, in Italy this right is limited to smart workers and is less extended than the French rule.

In Italy, the "smart workers" combine working from their office with working remotely to balance work and family commitments. As of mid-2019, there were estimated to be around 480,000 smart workers in Italy. Workers classified as "teleworkers" are covered by separate legislation that does not include the right to disconnect.[75]

Art 19 Law No. 81 of 22 May 2017 specifies that the agreement between worker and employer must regulate the rest periods of the employee and indicate the technical and organizational measures taken by the parties to secure the employee's right to disconnect from company's devices. The Italian legislator has followed to a certain extent the French approach and drafted the rule concerning the right to disconnect only as a framework leaving some aspects to the employer's requests or to mechanisms to ensure the employee's resting period.

In addition, sectoral and company-level collective agreements are in place, which tend to be extensive in their application. The sectoral coverage of such agreements is "high coverage – right to disconnect".[76] Company-level agreements include more detailed and operational provisions for individual smart working contracts. These provisions address for example the frequency of teleworking, core and flexible hours, the right to disconnect, and health and safety training. Examples in this regard are the

[72] Law No 191 of 16 June 1998 and Decree of the President of the Republic No 70 of 8 March 1999.

[73] Interconfederation Agreement of 16 July 2004 transposing the European Framework Agreement of 16 July 2002 and the Collective Agreement giving effect to it with the Framework Agreement of 23 March 2000.

[74] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 51.

[75] Ibid.

[76] Ibid, p 49.

agreements concluded by companies such as Eni (energy and oil), Poste Italiane (postal services), Italian State Railways (transport), Enel (energy), Barilla (agri-food) and Siemens (engineering).[77] Additionally, the banking sector expressing included the right to disconnect in the sectoral collective agreement of 2019.[78] This also provides the possibility for each employee to access a period of ten days of smart working per month.[79] In order to observe the requirements of a right to disconnect, the agreement establishes that the employees using company equipment must be guaranteed the right to rest, holiday periods, and leave entitlements. Further, outside agreed working hours and in cases of legitimate absence, workers are not required to access and connect to company information systems and may deactivate their own connection devices. The work-related communication has to take place exclusively through company devices and channels, with some exception – in the case of temporary or exceptional needs. UniCredit Italy goes a step further than the sectoral collective labour agreement and extends the right to disconnect to all employees working remotely in the company-level agreement.[80]

The share of remote workers has increased dramatically since the start of the COVID-19 pandemic in Italy and the government issued a decree establishing a simplified procedure for smart working that does not require individual agreements between employees and employers.[81] This approach, was originally expected to last until the end of January 2021, but it is set to remain valid until the end of the health emergency. After this, the collective labour agreements are expected to establish the details of the application of this right for smart workers.

For the public administration a Decree of 8 October 2021 of the Minister of Public Administration established the conditions for the return to in person presence of the employees of the public administration and those related to smart working. These guidelines are addressed to public administrations and other similar bodies required to provide for measures in the field of smart work, pending the regulation of national collective labour agreements for the period 2019-2021. The national collective labour agreements will regulate the institution for aspects not reserved to the decree. The guidelines provided by the Decree aim to definite the guarantees to secure transparent working conditions, which in turn are expected to favour productivity and be result orientated. Such guarantees are set to reconcile the needs of the employees with the organizational needs of the public administrations, allowing, at the same time, the improvement of public services and the balance between work and private life. With these guidelines the aim is to outline the way in which the so-called smart work performance is to be carried out having regard to the right to disconnect, the right to specific training, the right to the protection of personal data, trade union relations, the regime of

[77] Op. cit. *Working Conditions Right to Disconnect: Exploring Company Practices*, p. 20.

[78] Article 30.

[79] Article 11; see Chapter 1 for more information on the definition and regulation of smart working.

[80] See more details related to the agreement in op. cit. *Working Conditions Right to Disconnect: Exploring Company Practices*, p. 39-41.

[81] Article 87 Decreto-legge n.18 del 2020 as modified by Art 263 Decreto-legge n 34 del 2020.

permits and absences and the compatibility with any other institution of the employment relationship and contractual provisions.[82]

In Art 1(3) Decree establishes the requirements that have to be satisfied for using smart working. In accordance with Art 1(6) Decree, the conditions to be observed by the administration in relation to smart working relate to:

- The same quality of the services provided to the users regardless of whether this is provided by an employee working in presence or in smart working;
- The adequate rotation of staff authorised to carry out smart work while ensuring that priority is given to work in presence by each worker;
- Reliance on appropriate technological tools suitable to ensure the absolute confidentiality of the data and information processed during the performance of smart working;
- The need for the administration to provide a plan for handling backlog work, if accumulated;
- The provision of suitable electronic equipment for the employee;
- The conclusion of an individual agreement with the employee as referred to in Art 18(1) of Law No. 81 of 22 May 2017 which has to address:
    - The specific objectives to be attained when in smart working;
    - The methods and timeframe to carry out the work and eventually some time period when the employee can be contacted; and
    - The methods and the criteria to measure the performance of the employee also in view of continuing to engage in smart working practices;
- The prevalence for carrying out in presence work for employees carrying out coordination and control functions, managers, and persons in charge of various proceedings;
- Securing a rotation of the employees in person when this is required by health measures.

To accede to a smart working arrangement, both the employer and the employee must agree to such work relationship. This must be done in writing and establish the activities that the employee can carry out from outside the office premises, the instruments and devices necessary to carry out the activities and the way in which the employer is to exercise his power of direction.[83] The public administration entities are the ones that have to identify the activities that can be carried out via remote working arrangements. Further, it is considered that smart working should not be seen only as a work-private

[82] The guidelines will cease to produce their effects for the parts that will be incompatible with the new expected national collective labour agreement. See also Luca Catano, *"Schema di Linee guida in materia di lavoro agile nelle amministrazioni pubbliche, ai sensi dell'articolo 1, comma 6, del decreto del Ministro per la pubblica amministrazione recante modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni"*, Cammino Diritto (forthcoming 2022).

[83] Art. 19(1) Law No. 81 of 22 May 2017.

life balance tool and a way towards organisational innovation and modernising work procedures, but also as a way for the administration to reconcile the needs of well-being and flexibility of workers with the objective of improving the public service and taking into consideration the specific technical needs of the activities carried out.[84] The administration with the involvement of trade unions through the institutes of participation provided for by the national collective labour agreement, will take care to facilitate access to smart working arrangements for workers who find themselves in conditions of particular need, and who are not covered by other measures.

As timeframe constrains, the Italian provisions do not provide for any specific period during which the smart working tasks need to be carried out except that these have to be contained within the maximum of daily and weekly working hours established by the national collective labour agreement.[85] Furthermore, the time during which the employee cannot provide any work performance have to be properly identified. These periods concern the period which the employee is not operative (disconnected), thus, not performing any work-related tasks. This limitation includes the set period of eleven consecutive hours of rest.[86] Further, the right to disconnect is a mandatory element of the agreement that the parties have to execute to accede to the smart working regime, therefore its field of application is limited to smart workers, and thus, less extended compared to the French rule.

1.5.5 Germany

No specific legislation in relation to the right to disconnect was adopted in Germany yet, but German employers have made significant progress in self-regulating after-hours work that fit their business or industrial needs.[87] Teleworking or digital working practices are supplemented by sectoral and company-level collective bargaining agreements.[88] A white paper from the federal government found that there is no need for additional legislation to regulate the right to disconnect, as workers are not obliged to be available to their employers during their leisure time.[89] According to the paper the collective bargaining is perceived as the most appropriate means to regulate overworking and to protect the private life of workers from demands for flexibility. The German corporate self-regulatory approach allows employees to engage in discussions with the relevant social partners to develop unique regulations that are tailored to both parties.[90] This is based on the German work culture that values productivity and effective use of the employee's work time; thus, workers seek to deliver effectively during their work

[84] Op. cit. *"Schema di Linee guida in materia di lavoro agile nelle amministrazioni pubbliche, ai sensi dell'articolo 1, comma 6, del decreto del Ministro per la pubblica amministrazione recante modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni"* (forthcoming 2022).

[85] This is different from remote work that can also be performed with a time constraint and in compliance with the consequent attendance obligations deriving from the provisions of working hours, through a modification of the place of performance of the work performance which involves the performance of the service in a suitable place different from the office to which the employee is an employee.

[86] Art 17(6) Collective National Labour Agreement of 12 February 2018.

[87] Pascal R Kremp, *Employment and Employee Benefits in Germany: Overview*, Thomson Reuters Practical Law, 2017.

[88] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age,* New forms of employment series, p. 51.

[89] BMASK (2017), *Sozailbericht: Socialpolitische Entwicklungen und Maßnahmen 2015–2016*, Sozialpolitische Analysen, Vienna.

[90] Jeevan Vasagar, Out of Hours Working Banned by German Labour Ministry, Telegraph, 30 August 2013.

in order to guard their personal time, as separation between the two is essential to society.[91] The approach also encourages employers to develop regulations that serve their industrial needs.[92] And is considered to be better suited than having the legislator intervene and having to establish legislation that is either too simplistic or too detailed and difficult to apply or enforce.[93]

The Confederation of Germany Employers' Associations partnered with the German Trade Union Confederations and the Federal Ministry of Labour and Social Affairs to develop regulations that are suitable for the needs of both employees and employers.[94] Jointly known as "social partners", they collaborate to enact policies that are functional within specific industries, while still relieving pressures on employees.[95]

German employers recognise the harmful effects of constant pressure on their employees and companies such as Volkswagen, BMW and Puma have voluntarily imposed restrictions on when managers can e-mail employees outside working hours.[96] For example Volkswagen policy is not to forward any e-mails to an employee sent more than thirty minutes after the end of their working day.[97] This is deem to reflect both the needs of the employer who may need to contact an employee regarding something done at the end of the day, while also respecting the interest of the employee in preserving their time after work for activities not related to their employment. It appears that the company has also set its internal servers to refrain from sending emails to individual accounts between 18.15 and 07.00.[98] There are reports that also other companies have similar policies in Germany.[99] Further, there are also regional examples such as the agreement of the metal industry of Baden-Württemberg from 2018 that allows the reduction of the daily rest time of employees to nine consecutive hours instead of the usual eleven hours if during teleworking (*mobilen Arbeiten*) the employees can establish themselves the beginning and the end of their working day.[100] This is one of the examples in which a specific indication is given as to what should be the resting time during which employees should not be contacted. Metal industry collective agreement establishes more in detail that: (1) the employees are not entitled to mobile working; (2) there is no duty for employees to be available after the agreed working hours; (3) compliance with the statutory and collectively agreed working time regulations; and (4) working hours can be documented in detail or as a lump sum. If these requirements are met the overtime that is not agreed with the manager will not result in an payment of the overtime, and also if the employee is determining his working hours this will not be entitled to working late or right

[91] Op. cit. "The Employee Right to Disconnect", *Notre Dame Journal of International & Comparative Law*, 9(2019)1, Article 3, p. 30.

[92] Op. cit. *Working Conditions. Right to Disconnect: Exploring Company Practices,* p. 25.

[93] Colleen E. Medill, *Introduction to Employee Benefits Law: Policy and Practice,* 4th Edition, 2015, p. 70.

[94] Op. cit. *Employment and Employee Benefits in Germany: Overview.*

[95] Eurofound & International Labour Office [ILO] (2017), *Working Anytime, Anywhere: The Effects on the World of Work*, p. 48.

[96] Op. cit. *"The Employee Right to Disconnect"*, p. 29.

[97] Op. cit. "*Out of Hours Working Banned by German Labour Ministry"*, Telegraph, 30 August 2013.

[98] Op. cit. Eurofound, EurWORK, *Right to disconnect*, 22 October 2019.

[99] Op. cit. Eurofound, EurWORK, *Right to disconnect*, 22 October 2019.

[100] Op. cit. *The Right to Disconnect*, Briefing, p. 4; Tarifabschluss Mobiles-Arbeiten, Südwestmetall, 2018. Mobile Working - Südwestmetall (suedwestmetall.de)

surcharges.[101] When it comes to the analysis of the way such agreements are interpreted, scholars have argued that performing a work task during a period of information and communication technology-enabled availability outside contractual working hours should be considered working time and a break in the statutory rest period. However, at the same time, the interpretation of what is being "available" is more complex than it seems at first in a work world characterised by constant connection. Being "available" via information and communication technology and providing limited "favours" (e.g., a short exchange of information) is not considered a break in the statutory rest time.[102]

At the level of public institutions, the German Labour Ministry has itself adopted policies on after-hours communication to encourage other employers to follow. In this regard it has banned any communication with its employees outside the working hours, except for emergency situations, and implemented rules to prevent managers to take disciplinary action against employees who switch off their mobile devices or fail to respond to communication after working hours.[103] Hence, employees benefit from protection if they fail to reply or communicate after working hours

Although German employers are not bound to engage in corporate self-regulation, the corporate self-regulatory approach allows employees to engage in discussions with the relevant social partners with the aim to develop unique regulations tailored to the needs of each party. The risk involved in self-regulation, however, is that employers will often create rules that seemingly favour employees while yet in practice fail to give them substantive protection.

This self-regulatory approach is not welcomed by everyone in Germany. There have been some German lawmakers who criticized the present approach based on employers' initiatives and labelled them as insufficient. The general risk with self-regulation is that employers may create rules that at first sight seem to favour employees, but in fact fail to provide substantive protections.[104] It can be argued that employers may be incentivized to develop such rules to attract positive public reaction and employees.

It is difficult to quantify to what extent this identified industry practices have generalized or whether they have resulted in a significant shift as to limiting after-hours communication with employees nationally. There have been also calls to extent the ban on electronic communication with employees after hours in general, but for the moment no law has been adopted to regulate an employees' right to disconnect.[105]

1.5.6 The Netherlands

In the Netherlands, the Labour Law does not contain any express provisions on working from home or teleworking. In 2019 the Labour Party (*PvsA*) proposed a Law on the Right to Be Inaccessible (*"Wet op*

[101] Südwestmetall, Info Industry available at www.suedwestmetall.de/akkordeon/tarifabschluss2018/2018/02/mobiles-arbeiten.

[102] Hassler, M., Rau, R., Hupfeld, J., Paridon, W. and Schuchart, U. (2014), *Auswirkungen von ständiger Erreichbarkeit und Präventionsmöglichkeiten*, Report 23, Initiative Gesundheit und Arbeit, Berlin. See also op. cit. *Working Conditions Right to Disconnect: Exploring Company Practices*, p. 11.

[103] Op. cit. *"The Employee Right to Disconnect"*, p. 29.

[104] Martha Lagace, *Industry Self-Regulation: What's Working (and What's Not)?*, HARV. BUS. SCHOOL: RES. & IDEAS, 9 April 2007.

[105] Op. cit. *"The Employee Right to Disconnect"*, p. 30.

het recht op onbereikbaarheid"). It envisaged that implementation would take place through a strengthening of risk assessment, focusing on the risks associated with constant connection of employees.[106] An agreement would have to be reached between employees and employers in relation to the times when employees could not be contacted.[107] At present the Working Hours Law (*Arbeidstijdenwet*) contains rules on the working and rest time. For example, it has been determined that an employee of 18 years or older may work a maximum of twelve hours per shift and a maximum of 60 hours per week. The law also establishes that employees above 18 years of age must have a rest period of eleven hours (consecutive) after a working day. This rest period may only be reduced to eight hours once every seven days if the nature of the work or the operating conditions so require. However, if work-related messages are still sent during the eleven hours rest period, this is not a pure rest period.

A public consultation on the issue took place, which showed support for the initiative among the trade union movement. In this, the employers' organisations stated their preference for voluntary, tailor-made solutions at company level. According to the proposal, the Dutch legislator intents to leave the employers to reach an agreement with the employees regarding the rest periods and the right to be (un)reachable outside the working hours.[108] Employers would have a duty to map out the risks of being continuously accessible in their health and safety policy and the risk assessment and evaluation (*Risico-inventarisatie en evaluatie -RI&E*) and take measures to prevent the negative consequences of being reachable at all times. The aim is that if no occupational health and safety policy are followed or if nothing is recorded in the risk assessment and evaluation, the Inspection body of the Ministry of Social Matters and Work (*Inspectie SZW, Ministerie van Sociale Zaken en Werkgelegenheid*) should be able to issue a warning to the employer and then proceed to imposing a 'compliance requirement' and, subsequently, an administrative fine.

The current state of the advancement of the legislative proposal is not clear regarding the legislative agenda and significant disagreements on the issue remain between the social partners and political parties.[109] In anticipation of the entry into force of the law, the right to inaccessibility has already been included in the collective labour agreement for the care of the disabled. Employers who identify this problem within their company are advised to discuss it and possibly already implement a policy with regard to the (un)accessibility of employees outside working hours.[110]

1.5.7 Spain

On 7 December 2018, the Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights – *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los*

[106] On the risk for the workers and the pressure of being always connected see also S.S.S. M. Peters, *Baas over eigen tijd: Onbereikbaarheid als werknemersrecht*, TRA 2020/21.

[107] Arbowetweter, *Recht op onbereikbaarheid*, 7 April 2020.

[108] Art. I Voorstel van wet van het lid Gijs van Dijk tot wijziging van de Arbeidsomstandighedenwet in verband met het aangaan van een gesprek tussen werkgever en werknemers over bereikbaarheid buiten werktijd (Wet op het recht op onbereikbaarheid) (available at https://zoek.officielebekendmakingen.nl/kst-35536-2.html).

[109] Op. cit. *Working Conditions Right to Disconnect: Exploring Company Practices*, p. 18.

[110] Arbowetweter, *Recht op onbereikbaarheid*, 7 April 2020.

Derechos Digitales (LOPD)[111] – came into force in Spain. The law although geared towards creating the necessary framework for the application of the EU General Data Protection Regulation (GDPR) in Spain it also addresses so called "digital rights".

The new LOPD grants employees for the first time in Spanish legislation a right to digital disconnection (Art. 88 LOPD). As other national legislation analysed above the Spanish law leaves the details of the implementation of the right to disconnect to the adoption of subsequent collective agreements between parties at sector or company level.[112] According to the provisions of this law it is now compulsory for employers to establish a "digital disconnection policy". This ensures that the "digital detox" right is effectively guaranteed. According to LOPD, employees have the right not to be connected or available during rest times and holidays to ensure a proper work-life balance.

Spanish employers have to design a disconnection policy that guarantees the employees' right to digital disconnection in accordance with their position and builds a culture that respects the right to digital disconnection. As way of example, the disconnection policy can forbid the use of corporate email outside working hours, restrict the access to servers temporarily during certain timeframes, or limit the number of persons that can be copied on an email. Companies that have employee representatives must discuss the content of their digital disconnection policies with them. Although a positive step in terms of regulating this right, the LOPD does not set forth any specific penalties for breach of this obligation.

The disconnection policies to be adopted by employers are a good tool to avoid sanctions and claims regarding maximum working time and health and safety at work and can be seen as a new opportunity to regulate the uses of corporate email and corporate devices. Further, Art 87 LOPD expressly recognise the employer's right to access the devices to monitor and survey the employee's fulfilment of the contractual obligations and for the adequate use of the devices. Such to access to the devices used by the employee is recognised if the employer has clearly stated the conditions of use of the devices and if they offer a minimum standard of privacy. The employee representatives must participate in the process of establishing the conditions of use, which must be duly communicated to each employee. This is an important step towards creating a culture of data protection in the workplace and improving the employee's work-life balance.

Additionally, the LOPD sets out that future sector collective agreements have to include specific digital disconnection regulations. This has started to materialise in mid-2019 when the right to disconnect was included in the sectoral collective agreement in the manufacturing sector and in a number of agreements at sectoral or company level.[113]

[111] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20210527&tn=1#a8-9

[112] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age*, New forms of employment series, p. 51.

[113] Ibid.

1.6 Current Draft of Law on Digital Efficiency

Title I, Article 6 (entitled "*Derechos y deberes de los profesionales que se relacionen con la Administración de Justicia*"):

> Paragraph 2: "*In addition, with respect to the use of electronic means in judicial activity and in the terms provided for in this law, professionals who relate to the Administration of Justice have the following rights:*
>
> f*) That the information systems of the Administration of Justice enable and favour the digital disconnection, in a way that allows the reconciliation of work, personal and family life of professionals who relate to the Administration of Justice, with respect to the provisions of procedural legislation*
>
> *The Administrations with competences in matters of Justice must define, through agreements and protocols, the terms, means and appropriate measures, in the technological field, to enable disconnection, conciliation and rest in periods not working procedurally and in those in which the professionals of the Legal Profession, the Procura and the Social Graduates are making use of the possibilities provided for this purpose in the procedural rules."*

1.7 Comments and Recommendations

Currently, there is no common approach as to the way the right to disconnect should be regulated although some common lines can be identified in the Member States that have adopted dedicated provisions or are considering this step.

The outcome of the present fragmentation is that different levels of coverage can lead to inequalities between countries, sectors, or types of workers in terms of protection against the impact of technology on work–life balance and worker health. In regulating or seeking to regulate the right to disconnect, countries recognize the different needs of industries and public administration with regard to flexibility and resilience in case of prolonged emergencies as well as the need to secure a work-private life balance. Another positive consequence of having express provisions regarding a right to disconnect is that this is set to reduce the need of employees to seek to obtain similar results by relying on other provisions that are not specifically designed for teleworking. Additionally, the recognition of a right to disconnect sets the ground for the creation of technical tools as well as organisational practices that can support the exercise of the right to disconnect. Such solution can lie in the establishment of hard and/or soft means of disconnection (e.g., server or router shut down for a specific period, pop-up messages reminding employee they do not have to respond to emails after working hours or establishing a system of alerts for exceptional circumstances when the employees are requested to react).

Another aspect that needs to be addressed in connection to the right to disconnect is the issue of workload. This can be a sensitive element with public authorities that register and are seeking to address backlog with the implementation of technology. As underlined also by other studies "disconnecting without causing added pressure to the employee is only possible when workload and

working hours are sensibly aligned" otherwise there is a risk of constant pressure being put on teleworks to be available even after the working hours.[114]

Regulations in place have to be clear as to the working and non-working time. In relation to the judicial authorities there is not per se a need to address the right to disconnect from the perspective of the procedural rules or codes. To guarantee the minimum rest periods, rules or guidelines that establish the working time of the courts could be used also in relation to online environment. For example, for communication of procedural documents existing procedural rules can be accommodated to an online use. The same can be considered in the interaction between legal professionals and the courts. This means that for the party communicating the information the procedural timeframe can be considered uphold even when the document is transmitted after the usual office hours of the court or clerk office, while for the recipient there will be a duty to respond only from the next working day. If such option is deemed appropriate for the legislator, rules already in place for situations dealing with in person subjects can be extended to situations of online communications. In this case, no dedicated rules addressing different procedural circumstances will need to be adopted. This will avoid an additional layer of legislation and complexity as a result of different regimes being applicable between electronic and in person communication of procedural documents and/or to interactions between legal practitioners and courts. For this purpose, also technical solutions can be designed and integrated in the platforms used for communication. For example, solutions can be put in place to transmit or provide pop-up messages indicating the timeframe within which the communication will be reviewed/deemed communicated or providing for forwarding mechanisms or alternative access by other users when the original recipient is making use of the right to disconnect.

Alternatively, should a dedicated framework be deemed desirable, consideration should be first given to a more flexible approach such as a dedicated agreement between the legal professionals or at the level of the Ministry of Justice or the issuance of guidelines with regard to the timeframe of electronic communication for procedural purposes when these are carried out via information and communication technology means. This can mirror the timeframe and solutions used for in person procedures. The advantage of such solution would be that the practices are already familiar to all legal practitioners and will not create a fragmentation at the level of procedural rules applicable and legislation establishing such differences (e.g., between procedural rules and specific legislation addressing digital developments). Digitalisation should not be used to create an environment where legal practitioners and members of the court or court staff are connected at all times, but a dialogue should be encouraged to create a culture where boundaries are observed, or existing boundaries are recognized even in a digital environment and thus a positive work-private life balance can be maintained.

Lastly, should the first two solutions not be considered sufficient by the Spanish legislator a legislative action regarding civil procedure rules could be put in place to expressly address the situation. However,

[114] Op. cit. *Telework and ICT-based mobile work: Flexible working in the digital age*, New forms of employment series, p. 52.

an extensive legislative project should be taken only as a last resort given the close link of the right to disconnect to labour law rather than procedural law matters.

As a set of subsequent application norms to the provisions of Art 6(2)(f) of the Law on Digital Efficiency the following aspects may be considered for additional guidelines, professional agreements, or more detailed provisions:

- the communication between the judicial authorities and legal practitioners outside business hours/opening hours of the courts;
- use of reminders informing the sender that the message will only be reviewed on a specific day (e.g., next working day); and
- considering technical solutions of forwarding or giving access to several legal practitioners when the main recipient is making use of the right to disconnect.

2 Open Data

1.1 Introduction

For the purpose of this report and in order to ensure clarity, it is relevant to first make a distinction between several concepts that are sometimes used in an interchangeable way or be exchanged with each other. As pointed out by earlier research, there can often be a confusion between "access to information" and "access to data" (more precisely, access to information in the form of a database).[115]

On a general basis, a certain amount of information is considered useful and necessary for society and for this reason is provided to the public. To distribute this to the public, authorities rely on information technology. In the justice domain, such information can concern judicial statistics, legislation, case law, details about judicial authorities, appointments in various positions, information of public interest (e.g., e-Justice Portal, Légifrance.fr (France)). Although presented in a certain uniform way and having relevance, this information differs from data in a database that can be downloaded and processed by a computer or device to suggest solutions or "predict" outcomes of judicial authorities.[116] Thus, for the purpose of this report, data should be understood as a representation of information that can be used for automatic processing.

Open data can be simplistically defined as "data that can be freely used, re-used and redistributed by anyone".[117] In this context, it is referring to the creation of structured databases that are available for the public to consult and to download towards further use and re-use. For this, the data has to be legally and technically opened.[118] Data are legally open if existing licenses allow anyone to freely access, reuse, and distribute the data, while these are technically open if they are available in a machine-readable format and in bulk or raw for a price that is accessible (e.g. at a price of its reproduction).[119] "Open data therefore only involves the dissemination of "raw" data in structured computer databases".[120]

As a particular area of open data, the progress of opening judicial data to general use and re-use has been slower compared to data published by the legislative and executive branches of government.[121] Open judicial data is data that is produced by the judiciary and can be freely accessed, re-used, and redistributed. By opening the judicial data to the public it is expected that this can increase

[115] The data are meaningless letters and numbers. Information is data included in a context. It is the context that gives meaning to the data. We can guess that 2005 is a year, but without context, we do not know. But in "in 2005, we completed 3 projects" the context gives meaning to the number. Therefore, "open data" is not data in the sense of the definition, but information. Similarly, large data are also large amounts of information, not data. See European Commission for the Efficiency of Justice (CEPEJ), 2018. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 19.

[116] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 19.

[117] Open Knowledge (2017a). The open data handbook.

[118] For a more elaborated system of characteristics for opening data see Joshua Tauberer and Larry Lessig (2007), *The 8 principles of open data government* (available at http://opengovdata.org/).

[119] Marko Markovicand Stevan Gostojic (2018), *Open Judicial Data: A Comparative Analysis*, Social Science Computer Review, 20(10), p. 2.

[120] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 20.

[121] Op. cit. *Open Judicial Data: A Comparative Analysis*, p. 1.

transparency, participation, and collaboration of citizens and civil society, which in turn further access to justice.[122] These data can be used by the private sector to develop services for citizens, professionals as well as other branches of the government interested in specific information about justice and the judiciary activities (e.g., statistical data, judicial decisions in criminal matters, cases dealing with domestic violence, etc.). Internet available databases or online services related to the data can be thus provided to the public.[123] Making judicial decisions open data is a prerequisite for the development of search engines or trend analysis for the so called "predictive justice". However, processing this type of data raises a number of issues, among which the "changes in the formation of case-law and protection of personal data of professionals)".[124]

In terms of **data protection**, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract new and predictive knowledge for decision-making. Predictive justice using artificial intelligence, advanced search engines applying extremely precise criteria and legal robots are all algorithmic applications which are fed with data but have nothing to do with the policy of open data itself. However, the open data policy should be analysed in the light of the possibilities it offers for further processing, regardless of the nature of these processes. "If certain data are filtered upstream, taking account, for example, of the need for confidentiality and respect for privacy, subsequent risks of misuse appear to be reduced."[125] Further, these data can be re-used, likely in line with specific licensing terms for other databases.[126] "Open data should not be confused with unitary public information available on websites, where the entire database cannot be downloaded (e.g. a database of court decisions).[127] Further, it should not be considered that open data is to replace the mandatory publication of specific administrative or judicial decisions, or measures already laid down by certain national laws or regulations. Additionally, a confusion should not be made between data as open data and methods used to process it (e.g., machine learning) for different purposes (e.g., assistance in drafting documents, analysis of trends of decisions, predicting court decisions, etc.).[128]

1.2 Status Quo on Open Access Data

According to the analytical overview of the state of play on e-filing in selected member States of the Council of Europe, prepared in March 2021, "most countries guarantee proper information transparency on procedures and provide properly traceable digitized operations (i.e., transparent

[122] Op. cit. *Open Judicial Data: A Comparative Analysis*, p. 1.

[123] On the public interest to access court records see Natalie Gomez-Velez (2005), "Internet access to court records balancing public access and privacy", *Loyola Law Review* 51, 365–438.

[124] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 18.

[125] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 20.

[126] In this sense, it can be stipulated or prohibited that the public available data can be re-used for specific purposes or prohibited for certain other. See here also *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 73-74.

[127] "Analytical Overview of the State of Play in Electronic Court Filing (e-Filing)" Report, prepared by Giulio BORSARI, Alexandra TSVETKOVA and Harold EPINEUSE for CEPEJ-GT-CYBERJUST Working Group, final version dated 31st March 2021, p. 9.

[128] Ibid.

service delivery procedures and providing information about the process, including information on time, process, and delivery of the service), considering users' access rights and respective roles in a case".[129]

Court statistics are often accessible to public in most countries although the degree of detail of the data varies. These are usually collected by automatically retrieving data from case management systems or data warehouses. When it comes to court decisions available for public use, a common issue experienced by countries is the protection of personal data or sensitive information. In this regard, evidence for ongoing projects show a trend to develop tools for public case law databases to automatically or semi-automatically anonymize such personal or sensitive information. Additionally, the format in which court decisions are published is not always machine readable and in a format that can be automatically processed and/or reused. This is often the case with older decisions.

In consideration of these aspects that are relevant for the generation of open data by judicial authorities and their re-use, three EU countries were further analysed due to the development of their national legislation in this area, namely: Austria, Bulgaria, and France.[130]

1.2.1 Austria

Articles 15 and 15a of the Supreme Court Act establish that the full text as well as the abstracts (*Rechtssätzen*) of decisions of the Supreme Court are published in a general accessible database available on the Internet. An exception from publication are the cases in which an appeal is rejected without substantial reasoning.[131] In order to fulfil the requirements of privacy and sensitivity of certain data, in the text of the version published, names, addresses and, if necessary, other data that allow identification are anonymized by using letters, numbers or abbreviations in such a way that the meaning of the decision is not lost.[132] Article 15 of the Supreme Court Act contains two specific instructions in this sense: (1) in cases without a public hearing in all stages of the proceedings the Court can decide not to publish the decision if the anonymity of the person concerned cannot be guaranteed; and (2) personal data (e.g., names, addresses, other information) have to be anonymised in such a way that the transparency of the decision is not lost. Additionally, according to article 48a of the Judicial Organisation Act, decisions of other courts are to be published if their significance exceeds that of the individual case.[133] However, the text is not elaborated when this is considered to be the case. It is the court staff that establishes what is worth being published. As practice, the judicial decisions are

[129] Ibid.

[130] These three countries are the ones where regulations on open data are in place among the selected states for the report on "Analytical Overview of the State of Play in Electronic Court Filing (e-Filing)", prepared by Giulio BORSARI, Alexandra TSVETKOVA and Harold EPINEUSE for CEPEJ-GT-CYBERJUST Working Group, final version dated 31st March 2021.

[131] Article 15, Supreme Court Act, Federal Law Gazette No. 328/1968 last amended by Federal Law Gazette I No. 95/2001 (*OGH-Gesetz*), www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40020374/NOR40020374.html and www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40020375/NOR40020375.html.

[132] Article 15(4) Supreme Court Act, Federal Law Gazette No. 328/1968 last amended by Federal Law Gazette I No. 95/2001.

[133] Court Organization Act (*Gerichtsorganisationsgesetz*): www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40152363/NOR40152363.html.

published in full, with the particularity that the legal conclusions are made available in a separate file.[134] Most decisions are published within a few weeks since the court issued them. Prior to this, they have to be anonymised.

All published decisions are to be found on the Legal Information System of the Republic of Austria (*Rechtsinformationssystem des Bundes*, RIS).[135] The system is coordinated and operated by the Austrian Federal Chancellery (*Bundeskanzleramt*) and provides access to anonymized court decisions via a service application programming interface (API), and a mobile application called RIS:App. In contrast the court cases register data are not opened to the public. The full court decisions are available in XML, HTML, PDF, and RTF formats. The *Judikatur Justiz* database contains decisions of the civil and criminal courts as well as from the Supreme Patents and Trademarks Boards (*Obersten Patent- und Markensenats*).[136] Separate databases exist for the Constitutional Court,[137] the administrative courts,[138] the High Administrative Court,[139] and the Federal Administrative Court.[140] The database of the Federal Financial Court is hosted on its own website.[141] Besides the decisions of the Supreme Court and some Courts of Appeal that are available for consultation, almost 100,000 decisions of 1st instance courts are available for internal users. The aim is to continue publishing them when the ongoing project for automatic or semi-automatic anonymization of court decisions will reach an adequate degree of reliability. Further, all court decisions have to be provided in the available format and language and as far as possible in open and machine-readable format together with the associated metadata according to §6 Federal Law on the further Use of Information from Public Bodies. In practice the court decisions published on RIS are available for re-use via FTP.[142] However, the law does not oblige public authorities including courts to create new documents or to adapt them or to provide extracts from documents if this involves a disproportionate effort that goes beyond simple processing.[143] In general, there are no restrictions in the re-use of the decisions published, except for those on data protection requirements that derive from the Federal Act on the Re-use of Public Sector Information.[144] For using the data, a request has to made in writing to the authority concerned who has in its possession the requested documents.[145]

[134] Decisions have been published since 2000; the oldest decision being from 1905.

[135] Available at https://www.ris.bka.gv.at/Judikatur/. See also https://www.ris.bka.gv.at/UI/Erv/Info.aspx.

[136] https://www.ris.bka.gv.at/Jus/.

[137] https://www.ris.bka.gv.at/Vfgh/.

[138] https://www.ris.bka.gv.at/Lvwg/.

[139] https://www.ris.bka.gv.at/Vwgh/.

[140] https://www.ris.bka.gv.at/Bvwg/.

[141] https://findok.bmf.gv.at/findok?execution=e1s1.

[142] §§ 1-2 Federal law on the further use of information from public bodies (*Informationsweiterverwendungsgesetz*), Federal Law Gazette I No. 135/2005: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004375.

[143] §6(2) Federal law on the further use of information from public bodies (*Informationsweiterverwendungsgesetz*).

[144] §3(1) Federal law on the further use of information from public bodies (*Informationsweiterverwendungsgesetz*).

[145] §5(1) Federal law on the further use of information from public bodies (*Informationsweiterverwendungsgesetz*).

Empirical research carried out with regards to e-filing revealed that the Austrian systems guarantee proper information transparency on procedures. The systems also provide properly traceable digitized operations (i.e., transparent service delivery procedures and information about the process, including information on time, process, and delivery of the service).[146]

Court statistics are accessible online. Some registers (particularly, business and land ones), under the control of the Austrian Ministry of Justice, are published also as open data. Along with annual statistical data provided via the website of the Austrian Ministry of Justice ,[147] there are annual reports of the Supreme Court. Both this information is published in PDF format with no open license information.[148]

1.2.2 Bulgaria

The main legal act regulating the right of access to public information in Bulgaria, as well as to the re-use of public sector information is the Public Access to Information Act. It was adopted in 2000 and incurred several amendments during the years.[149] According to Art 4 of this law, any Bulgarian citizen as well as any foreigner or stateless person or legal person have the right to access public information and the right to re-use data published by public authorities. However, the use of the right of access to public information and the re-use of public information have some limitations. They should not be exercised in a way that touches upon the rights and good name of other people, as well as against national security, public order, public health, morality, classified information or other protected secrecy as provided for by law.[150] Further, each public authority has a duty to plan annually the gradual publication in an open format on the internet of the data sets and resources it maintains.[151] Access to these data is mainly free.[152] The public authorities are set to publish these data on the Open Data Portal managed by the e-Government State Agency.[153] Subsequently, the e-Government State Agency has to draft a public report every three years on the availability of information for re-use provided by public sector bodies, the conditions under which it is provided and the practices of redress.[154]

According to Art 41a of the Public Access to Information Act, data is to be provided in a format and in the language in which it was created or in another format at the discretion of the public authority and in an open, machine-readable format, together with the relevant metadata. The creation, maintenance and provision of information is to comply with the principle of "open by design and by default".[155] Public

[146] Op. cit. *Analytical Overview of the State of Play in Electronic Court Filing (e-Filing) Report*, Appendix 2 "Country report – Austria", p. 3.

[147] https://www.justiz.gv.at/home/justiz/daten-und-fakten/taetigkeit-der-gerichte-und-staatsanwaltschaften.1e6.de.html.

[148] https://www.ogh.gv.at/medien/taetigkeitsberichte/.

[149] Art 1 Public Access to Information Act (available at https://lex.bg/bg/laws/ldoc/2136867758).

[150] Art 5 and 7 Public Access to Information Act.

[151] Art 15b Public Access to Information Act.

[152] Art 8(1) Ordinance on the Standard Conditions for the Re-use of Public Sector Information and for Its Publication in Open Format (available at https://lex.bg/bg/laws/ldoc/2136867758).

[153] Art 15d Public Access to Information Act. Article 2(1) Ordinance on the Standard Conditions for the Re-use of Public Sector Information and for Its Publication in Open Format.

[154] Art 16a Public Access to Information Act.

[155] Art 4(2) Ordinance on the Standard Conditions for the Re-use of Public Sector Information and for Its Publication in Open Format.

authorities do not have a duty to provide information for re-use where this requires its creation or adaptation or where it relates to the provision of parts of documents or other materials, which requires a disproportionate amount of effort going beyond the normal operation. At the request of the applicant, and if possible, the requested information shall be provided electronically to the e-mail address or by other appropriate means for providing the information in electronic form. However, certain type of information that is for example protected by a third party's intellectual property rights, scientific and research organizations, information containing statistical secrecy collected and stored by the National Statistical Institute or by a body of statistics, information of an overriding public interest, information containing personal data the reuse of which constitutes inadmissible access or inadmissible processing of personal data according to protection requirements, and use of data would lead to unfair competition, will not be provided for re-use according to Art 41b of the Public Access to Information Act. For public authorities generated data will be made available for re-use upon the submission of a written request that can be made also electronically (Art 41e(1) of the Public Access to Information Act).

An ordinance - Ordinance on the Standard Conditions for the Re-use of Public Sector Information and for Its Publication in Open Format - was adopted in June 2016, hence several years after the adoption of the Public Access to Information Act.[156] The rules lay down the standard conditions for the re-use of public sector information and for publication of public sector information in an open format for commercial or non-commercial purposes.[157] The access to the information files, the data sets and the resources is to be in a free, open machine-readable format that allows reuse.[158] Furthermore, the ordinance prescribes the rights for free re-use, processing and distribution of courts' acts in compliance with the requirements of the Bulgarian Personal Data Protection Act and of the Classified Information Protection Act.[159] If a fee is applicable this is to be determined by costs of the performance[160] to cover a significant proportion of the costs associated with the collection, production, reproduction and dissemination of information. In accordance with law, or established administrative practice, the payment duty is set to established in advance and published electronically. The amounts collected from the fees of re-use of information will become part of the budget of the public authority concerned.

Art 64 of the Bulgarian Judiciary Act establishes that court acts, except for those in criminal cases by which the defendant is sentenced to serve a sentence, are to be published immediately after the ruling given by the court on its website in compliance with the requirements of the Personal Data Protection Act and of the Classified Information Protection Act and preventing the identification of national

[156] Ordinance adopted by the Council of Ministers № 147 of 20.06.2016, prom. State Gazette, no. 48 of June 24, 2016, amended and extended by State Gazette, no. 60 of July 7, 2020.

[157] These conditions may not impose unnecessary restrictions on reuse possibilities or restrict competition, Article 41a(5) Public Access to Information Act.

[158] Art 2(2) in conjunction with Art 5(2) Ordinance on the Standard Conditions for the Re-use of Public Sector Information and for Its Publication in Open Format.

[159] Art 41e Public Access to Information Act in conjunction with Art 11(1) paragraph 3 Ordinance on the Standard Conditions for the Re-use of Public Sector Information and for Its Publication in Open Format.

[160] Art 41g Public Access to Information Act.

persons. The same is the case for enforcement decisions.[161] At present, the case-related information and documents are available via the national e-Justice portal. Although the national e-Justice portal is operative, there is no (fully) automated case tracking or procedural overview of cases in place yet. The secondary legislation regulating the register of judicial decisions was adopted by the Bulgarian Supreme Judicial Council in 2017.[162] According to the Ordinance on the Keeping, Storing, and Access to the Register of Judicial Decisions, the Register of Judicial Decisions is set to be designed as a web-based electronic database to comprise every formal adjudication on the substance of a case and all judicial acts closing or ceasing any further judicial proceedings. Art 29 of the Ordinance obliges the Supreme Judicial Council to provide access to the entire database of court decisions or structured parts thereof in accordance with the applicable rules for accessing public information and re-use of information from the public sector.[163] Such database is to be public and available in free access in accordance with Art 26.[164] The technical standards for providing access to the register, including the type of electronic documents used and file formats, are to be published on the Supreme Judicial Council and on the website of the register in accordance with Art 11. However, this is not possible at the moment as the rules related to publication have not been published yet; thus, the technical solutions are not yet available.

With regard to the treatment of privacy or sensitive data, as a general outcome, all court decisions are publicly available after being anonymised. Anonymisation is carried out in a semi-automated process. Designated rules on personal data to be anonymized are part of the secondary e-justice legislation. Limitations (publication of partial information, no publication) are introduced only with respect to legal constraints (e.g., procedural rules, protection of classified information, tax issues, bank secrecy, etc.); in practice each court is left the discretion to decide on these specificities, while waiting for the Supreme Judicial Council to unify what information is not to be published.[165]

When it comes to open access, as said, the Bulgarian Supreme Judicial Council has to provide access to the entire database of court decisions or structured parts thereof in accordance with the applicable rules for accessing of public information and re-use of information from the public sector. The register of court decision should provide information on the decision issued, a description of the merits of the case, and indication of the stage of the proceedings or whether the decision is subject to an appeal or is final.[166] According to Art 4(1) Ordinance on the Keeping, Storing, and Access to the Register of Judicial

[161] Available at https://www.lex.bg/laws/ldoc/2135560660.

[162] Art 360t Judiciary Act in conjunction with Ordinance No 4 from 16 March 2017 on the Keeping, Storing, and Access to the Register of Judicial Decisions, prom. State Gazette, No. 28 from 04.04.2017 (available at http://www.vss.justice.bg/root/f/upload/14/Naredba4.pdf).

[163] Such dedicated rules have not yet been adopted and there are some practical difficulties related to the ongoing integration between the systems used.

[164] For the details related to publication in the register and category of information provided see Art 7-16 Ordinance No 4 of 16.03.2016 on the Keeping, Storing, and Access to the Register of Judicial Decisions, prom. State Gazette No. 28 of 04.04.2017 (available at http://www.vss.justice.bg/root/f/upload/14/Naredba4.pdf). Attention should be given to the fact the Ordinance has not been yet amended following the changes in 2019 to Article 64 Judiciary Act.

[165] Op. cit. *Analytical Overview of the State of Play in Electronic Court Filing (e-Filing) Report*, p. 10.

[166] Art 2(1) Ordinance No 4 of 16.03.2016 on the Keeping, Storing, and Access to the Register of Judicial Decisions.

Decisions this is available online in a web-based format. The database is part of a unified and centralised information system of the courts that secures the integrity, accessibility and security of the information contained in the court decision registry; yet, some practical difficulties remain considering the undergoing integration between existing systems used.[167] This is because the case tracking and procedural overview of the Bulgarian case law is not yet fully automated, there is no single database (no single access therein), and the portal does not cover the requirements of the Ordinance with respect to the type of information to be published per decision.[168]

When it comes to the re-use of the case law databases data, there are no legal restrictions applying and there are not technical facilities to support the access per se (see above),[169] so re-users have to find their own technical solutions. Furthermore, the re-use of the lower court decisions cannot be carried out in an automated way as download in bulk of the data is not possible since every download is protected by a Captcha solution.[170] For re-using these data a manual process of collection of the decisions would be necessary.

The Bulgarian **court statistics** are not published in an automated way. Only certain categories of court statistics are published, and they provide an overview over 6-month periods on the website of the Supreme Judicial Council. The data published on the website of the Supreme Judicial Council are the result of a manual handling of the data and are in principle available also in a machine-readable format.[171] However, the Council stopped publishing the data in a in machine-readable format in 2017.[172]

A dedicated specialized information system for the monitoring and analysis of judicial data is currently being developed and it is expected to enhance and automate judicial statistics (for all judicial authorities) as well as the assessment of the courts workload. This was expected to be ready by the end of 2021 but has not been launched yet.[173]

[167] Art 4 Ordinance No 4 of 16.03.2016 on the Keeping, Storing, and Access to the Register of Judicial Decisions.

[168] See https://legalacts.justice.bg/ and op. cit. *Analytical Overview of the State of Play in Electronic Court Filing (e-Filing) Report*, Appendix 3 "Country report – Bulgaria", p. 3-4.

[169] Op. cit. *Analytical Overview of the State of Play in Electronic Court Filing (e-Filing) Report*, Appendix 3 "Country report – Bulgaria", p. 3-4.

[170] Marc van Opijnen, Ginevra Peruginelli, Eleni Kefali, Monica Palmirani, *On-line Publication of Court Decisions in the EU*, Report of the Policy Group of the Project "Building on the European Case Law Identifier", 2017, p. 65 (available at https://bo-ecli.eu/uploads/deliverables/Deliverable%20WS0-D1.pdf).

[171] See http://www.vss.justice.bg/page/view/1082.

[172] See http://www.vss.justice.bg/page/view/7820.

[173] See technical specifications: http://profile-op.vss.justice.bg/?q=page&idd=index&porachkaid=20200410bwZc3342763

1.2.3 France

In France, the government's Légifrance website is the main online source of certified public information.[174] The website comprises not only French legislative and regulatory texts and case-law, but also European legislation and cases law, parliamentary debates, collective agreements, administrative documents, and information on appointments to public posts. This unitary information access point, although available on the Internet, differs completely from direct access to data organised and included in a database that can be downloaded and processed by a computer system.[175] Re-use of court decisions published on Légifrance is allowed, and facilitated by an FTP connection offering XML files.[176] A general Open Licence is applicable,[177] but an additional statement has to be produced to prevent re-users from re-identifying anonymised data subjects.[178] The internal databases maintained by the Court of Cassation, are only accessible on subscription. They can be used for example academic research or other re-use, but the subscription contract imposes strict rules on the anonymisation of any document from this database if disseminated. The Council of State also offers a licence for more detailed information from its database, but without any right to re-use.

With regard to dedicated legislation on open data, a law was enacted in 2016. The Law for a Digital Republic (*Loi pour une République numérique*) imposes a compulsory framework for the open data dissemination.[179] The major innovative aspect of this law that entered into force on 7 October 2018 is that is sets the principle of open data "as a principle" and introduces the obligation for communities with more than 3,500 inhabitants and administrations with more than 50 agents, to publish online their databases and data whose publication is of economic, social, health or environmental interest. Until now, some of these documents could only be disseminated subject to anonymization of the personal data that may appear therein. Following this law, documents containing personal data that do not infringe the privacy of the persons concerned can be published as open data.[180]

On court decisions, articles 20 and 21 of the Law for a Digital Republic brake away from previous practices that required a selection of decisions of the judicial and administrative courts to be made for dissemination based on their characterisation as being "of particular interest".[181] These articles modified Article L111-13 Code of judicial organisation and Art L10 of Administrative justice to establish

[174] www.legifrance.gouv.fr. Décret n° 2002-1064 du 7 août 2002 relatif au service public de la diffusion du droit par l'internet (available at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000413818/).

[175] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 19.

[176] Op. cit. *On-line Publication of Court Decisions in the EU*, Report of the Policy Group of the Project "Building on the European Case Law Identifier", p. 88.

[177] https://www.etalab.gouv.fr/wp-content/uploads/2014/05/Open_Licence.pdf

[178] Details of the CNIL on the Opening of Legifrance Case Law Datasets (*Précisions de la CNIL sur l'Ouverture des Jeux de Données de Jurisprudence de Légifrance),* available at https://www.eurojuris.fr/articles/precisions-de-la-cnil-sur-louverture-des-jeux-de-donnees-de-jurisprudence-de-legifrance-35865.htm.

[179] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

[180] See https://www.numerique.gouv.fr/espace-presse/loi-pour-une-republique-numerique-parution-du-decret-fixant-les-categories-de-donnees-diffusables-sans-anonymisation/

[181] Article R111-10 Code of judicial organization; Article R433-3 Code of judicial organization; Art R433-4 Code of judicial organization.

that all judgments are public and have to mention the name of the judges that issued them. They all have to be made available for the public free of charge and respect aspects of privacy of the persons concerned.

With regard to the identification of the name of the professional in the decisions published in open data, discussions took place seeking to reconcile what are often seen as conflicting requirements: (1) making public activities transparent by allowing citizens to know and evaluate their judges and (2) protecting the privacy of professionals (whose functions should not limit their fundamental guarantees in this field). Guaranteeing the impartiality of the judges and even of judicial institutions as a whole may be challenging even if the data policies are actually designed to meet them.[182] One of the important questions raised was what practical measures could be taken to protect them from potential attempts to destabilise the judiciary by cross-reference to judges' personal data in databases with other sources (social networks, commercial sites) to try to identify hypothetical political, religious and other biases.[183] The response in France was not clear cut as there was no clear side recommendation of prohibiting publication but reserving it for certain types of litigation and ruling it out for others (for example, for specialised criminal matters). The possibility of publishing only the names of the Court of Cassation judges was proposed, although it was conceded that this might result in an imperfect solution.[184]

For privacy requirement, an analysis is to be carried out prior to publication of judicial and administrative decisions to identify if there are risks of re-identification of the persons involved.[185] Publication of decisions is to be carried out only after this risk has been mitigated. However, it appears that a fully effective automated post-identification mechanism that can prevent any risk of identification or re-identification has not yet been devised.[186]

The broad publication of decisions is expected to lead to a greater awareness of judicial activity and case law trends, and thus, increase the quality of a justice system and the creation of a completely new factual reference base.[187] However, this process has to be carried out with some care and should be placed in the context of the principles set out by the European Court of Human Rights in case of differences in domestic case-law. The Court clearly emphasises the need to balance legal certainty, which makes decisions more predictable, against vitality and evolution in judicial interpretation.[188] To this, consideration should be given also to technical aspects such as the fact that the collection of all judicial decisions eligible for publication is not necessarily well co-ordinated between all levels of courts: particularly as regards first instance decisions.

[182] ECHR *Previti v. Italy*, No. 45291/06, §§ 249 et seq., which recalls the principles of objective impartiality of the judge.

[183] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 28.

[184] Study by Professor Loïc Cadiet. *L'Open Data. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice*, November 2017, p 43-50 (available at https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000019.pdf).

[185] Article R111-12 Code of judicial organization; Article L10 Code of administrative justice.

[186] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, § 35.

[187] Op. cit. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, p. 19.

[188] *Greek Catholic parish Lupeni and Others v. Romania* [GC]. No. 76943/11, 29/11/2016, § 116.

Although the law requires all French court decision to be accessible online for all instances as a result of an open data obligation, a recent obligation imposing anonymization appears to have slowed down the process and delays are expected. This longer timeframe is also influenced by the increased volume of court decisions from all instances (first instance to Court of Cassation) that need to be processed and should be completed in the coming years.[189] This is why an Order of the French Ministry of Justice of 28 April 2021 established a calendar to gradually achieve this as follows:[190,191]

- For the administrative courts, decisions are to be made available to the public and issued to third parties at the latest at:
  - 30 September 2021 with regard to the decisions of the Council of State;
  - 31 March 2022 with regard to the decisions of the administrative courts of appeal;
  - 30 June 2022 with regard to decisions of administrative courts.
- For civil, commercial and social disputes falling within the jurisdiction of the judicial order, all court decisions are to be made available to the public and issued to third parties no later than:
  - 30 September 2021 with regard to the decisions rendered by the Court of Cassation;
  - 30 April 2022 with regard to decisions rendered by the courts of appeal;
  - 30 June 2023 with regard to decisions rendered by industrial tribunals;
  - 31 December 2024 with regard to decisions rendered by commercial courts;
  - 30 September 2025 with regard to decisions rendered by the courts.
- For criminal disputes falling within the jurisdiction of the judicial order, all court decisions are to be made available to the public no later than:
  - 30 September 2021 with regard to the decisions rendered by the Court of Cassation;
  - 31 December 2024 with regard to decisions rendered by the courts of first instance in contravention and tort matters;
  - -31 December 2025 with regard to the decisions rendered by the courts of appeal in matters relating to contraventions and tort;
  - 31 December 2025 with regard to decisions rendered in criminal matters.
- Litigation of particular public interest from these above categories, as determined by the Ministry of Justice, will be made available to the public prior to the dates indicated above.

[189] See further on this sub-section 3.6.1. below on the EC study on the use of innovative technologies in the justice field.

[190] https://www.legifrance.gouv.fr/loda/id/LEGIARTI000043427953/#LEGIARTI000043427953.

[191] Order of 28 April 2021 made pursuant to Article 9 of Decree No. 2020-797 of 29 June 2020 on the making available to the public of decisions of judicial and administrative courts, NOR: JUST2111743A, JORF n°0101 of 29 April 2021.

This means that the first step of providing open data in relation to judicial and administrative decisions has been made with the provision of the decisions of the Court of Cassation and the Council of State becoming available on their respective websites. These decisions have become available on their websites since the end of September 2021.[192] To support this process, the website of the Ministry of Justice makes available online a dedicated portal presenting all access links, but also a complete file with the key questions of open data of court decisions as well as information on the remedies available to exercise their rights. Both databases are equipped with new search function and correspond to the requirements set by the law, which is more protective of the privacy and security of the persons mentioned in the decisions than the previous regime, thanks to a new mechanism for concealing the personal data of the persons mentioned in the decisions.[193] In addition, in parallel with this open data platform, administrative court decisions considered of interest are posted online daily on the website of the Council of State - Ariane web.[194] The Court of Cassation implemented the Judilibre system to make available to the public, free of charge, an open database of the decisions of the Court of Cassation, possibly enriched and pseudonymized. According to the schedule established by the decree of 28 April 2021, this database is to be extended with decisions rendered by other jurisdictions of the judicial order. Thus, as of 30 September 2021, approximately 480,000 decisions issued by the Court of Cassation, mainly since 1947, are available in the Judilibre database.[195] Some decisions rendered previously can also be found there. The decisions are entered in the Judilibre database on the same day of their delivery for judgments published in the Bulletin (judgment B) and within a maximum of one week after their delivery for other judgments of the Court of Cassation. In addition numerous supplementary information about the decisions may be made available in the database: the titles and summaries of the published judgments, certain preparatory works (reports and opinions of the Advocates General), documentary references, the appended means of the rejection decisions not specifically reasoned, comparisons of case-law, references to the texts applied, references to the decision which was the subject of the appeal before the Court of Cassation or, where applicable, the appealed decision itself if this decision has already been made public and has been pseudonymized.

Next, the decisions issued by the administrative courts of appeal as well as those rendered by the courts of appeal of the judicial order in civil, social, and commercial matters will be posted online, respectively in March and April 2022. Further, an investigation by the Ministry of Justice was opened until 30 November 2021 to better understand the use and re-use of data resulting from the published decisions. Results are not yet made available.

[192] Administrative justice is committed to opening and making all of its court decisions available in open data. In accordance with the Law n° 2019-222 of March 23, 2019, of 2018-2022 programming and reform for justice. https://opendata.conseil-etat.fr/.

[193] On the anonymisation of the data see Décret n° 2020-356 du 27 mars 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé "DataJust" (available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041763205).

[194] This site has sophisticated consultation functions and offers the users the possibility to download these decisions considered of interest in html format. See https://www.conseil-etat.fr/ressources/decisions-contentieuses/arianeweb2.

[195] https://www.courdecassation.fr/acces-rapide-judilibre.

It is to be noted that French initiatives to date to re-use such open data are essentially private and generally target professionals such as lawyers or legal departments of various organisations.

According to empirical research carried out with regards to e-filing,[196] court statistics in France are very basic, running on local databases court-by-court, procedure-by-procedure. At national level statistical data gathered by the Ministry of Justice is published on a dedicated page of the Ministry of justice. The statistical data is published subsequently in three-month format or yearly reports concern main areas of law such as civil and commercial, administrative, criminal, minors, or professionals.[197] Besides the published statistical data, the Ministry of Justice may collect specific information in relation to specific procedures but does not publish all the data available it in the general open access reports. An example in this regard is the application of the European Uniform Procedures by the French courts.[198] It is expected that the new systems established by the Council of State and the Court of Cassation will be able to provide more accurate court statistics in real time especially with respect to information that is currently not available for open consultation.

1.3 Current Draft of Law on Digital Efficiency

The current draft contains the following general provision:

- Title III, Chapter II, Article 35 (entitled "Principio general de orientación al dato"):

  Paragraph 1: "*All information and communication systems used in the field of the Administration of Justice, including for governmental purposes, shall ensure the entry, incorporation and processing of information in the form of metadata, in accordance with common schemes, and in common and interoperable data models that enable, simplify and favour the following purposes: …*" letter i): "*information to open data portals in the form to be determined*"

The whole Title VI is dedicated to this topic:

- Article 83 (entitled "Del Portal de datos de la Administración de Justicia"):

  Paragraph 1: "*The Data Portal of the Administration of Justice will provide citizens, citizens and professionals with processed and accurate information on the activity and workload, as well as any other relevant data, of all courts, judicial offices and prosecutor offices, provided by the Justice systems in the terms defined by the State Technical Committee of the Electronic Judicial Administration, in order to reflect the reality of the Administration of Justice with the greatest possible rigor and detail*"

[196] Op. cit. *Analytical Overview of the State of Play in Electronic Court Filing (e-Filing) Report*, p. 9.

[197] http://www.justice.gouv.fr/statistiques-10054/.

[198] Regulation (EC) No 1896/2006 creating a European order for payment procedure, OJ L 399, 30.12.2006, p. 1–32 and Regulation (EC) 861/2007establishing a European Small Claims Procedure, OJ L 199, 31.7.2007, p. 1–22. See for example on this Elena Alina Onţanu, *Cross-Border Debt Recovery in the EU. A Comparative and Empirical Study on the Use of the European Uniform Procedures*, Intersentia, 2017, p. 146 and 149.

Paragraph 2: "*The National Commission for Judicial Statistics shall determine the judicial statistics information which, for the purposes provided for in the preceding paragraph, shall be published on the Portal.*"

Paragraph 3: "*Within this Portal will be included a section where the information will be considered "open data*"

- Article 84 (entitled "Sobre las condiciones y licencias de reutilización de datos")

  Paragraph 1: "*The data, requests and licenses for the reuse of data, which in compliance with the provisions of the previous article were published in the open data section, will be subject to the provisions of Directive (EU) 2019/1024 of the European Parliament and of the Council, of June 20, 2019, on open data and the reuse of public sector information, and in Law 37/2007, of 16 November, on the re-use of public sector information, and will be considered "open data" according to that Directive*"

- Article 85 (entitled "Datos automáticamente procesables")

  Paragraph 1: "*The Administrations with competence in matters of Justice will ensure that the data published in the Data Portal of the Administration of Justice are automatically processable whenever possible. To this end, the computer systems of procedural management of the Administration of Justice and its associated applications must allow the automated extraction of the data necessary for the preparation of public information from the portals. It will be, in any case, the responsibility of each Administration with competences in matters of Justice to provide the data in ideal conditions for its use in the information of the web portals*"

1.4 Focus on anonymized decisions

Court decisions are published with more consistency and with more elaborated selection criteria if a legal framework is setting a duty on the judiciary or another public body to do so – or if a detailed policy guideline – exists. A general distinction can be made between Eastern-European EU countries, where the publication is often prescribed by a very detailed legal framework, and Western-European EU countries, where a legal framework is absent or only exists in policy guidelines.

In those EU Member States without a detailed legal framework, most often a selection of case law considered relevant is made. The selection process is mostly left to the judge or a judiciary department, but clear rules on what should be selected are often absent or too vague. In absence of a national legal framework, Recommendation R(95)11 of the Committee of Ministers of the Council of Europe offers guidance on what should be published.

However, notable differences regarding anonymization of court decisions can be found not only between the EU Member States but also within the Member States themselves, depending on the legal and policy framework and selection rules in place.

Also, legal and policy frameworks in most EU Member States provide for specific rules in balancing public and private interests, which are dependent on the specific types (nature) of decisions and/or

proceedings and are also reflected in the anonymisation provisions established. The difference rests in the level at which the legal or policy framework is detailed. In some Member States even the method that must be used for anonymisation is prescribe (i.e., obscuring, replacement by initials, fake data, or roles), while in others only the goal is established (e.g., not making the text illegible).

In the context of the huge variety of court decisions, where personal data should be anonymized, Member States lack - to some extent - uniform understanding which data should be considered personal data and should be anonymized in terms of protection of privacy. This has improved with the enforcement of the GDPR, but differences still exist, as the overall development of this sub-field falls behind the dynamic nature of the privacy rules and guidelines.

Other problems lie with the different structure of the court decisions across jurisdictions (in terms of both geography and type of law), the quality of the data and its machine readability (in most cases the national judicial practices and/or rules do not fully comply with the PSI Directive prescriptions), etc.

1.5 Comments and Recommendations

The main finding is that, despite existing regulations on open data and re-use of public sector information, only a limited number of countries publish judicial data in an open (and possibly machine-readable) format.

All three countries examined have decided to provide decisions in open data format with Bulgaria and France providing the whole database, while Austria – a limited selection made by court staff. The main obstacle regards the need to anonymize the text, for which fully automatic solutions (also based on machine learning techniques) are still under development and have not reached yet an adequate degree of reliability. Hence, at present, a certain effort for human intervention is needed.

Another issue, still under debate in France, is related to names of practitioners (especially judges) published in open data, and the need to protect them from potential attempts to destabilise them by cross-reference with other sources like social networks to try to identify hypothetical political, religious, and other biases.

In the current draft of the Spanish Law on Digital Efficiency, general provisions on open data are already in place, also regarding conditions and license for re-use and the need to provide machine-readable data. The content to be published is related to two main areas: (a) activity and workload, as well as "any other relevant data […] in order to reflect the reality of the Administration of Justice", and (b) judicial statistics. It seems that decisions are excluded.

On the contrary, if decisions are to be considered included, recommendations are given hereafter to add provisions in a secondary level legislation:

- decisions are published in open data in such a way that the privacy of the persons concerned is not infringed
- measures to avoid the re-identification of anonymised data subjects are to be put in place

- as both Austria and Bulgaria explicitly refer in their laws to public authorities (including courts) not being obliged to create new documents or to adapt them or to provide extracts from documents if this involves a disproportionate effort that goes beyond simple processing and normal operation
- the law should provide a clear format as to the information to be provided or anonymised, as well as to provide the respective rules for such publication or anonymization, in order to ensure uniformity between courts in the publication of cases and a better quality of the data to be subsequently used in various forms of automated handling or processing.

Considering the concerns highlighted above, decision needs to be taken if the names of the judges are to be left in the published data. Some legislations – like in Bulgaria – establish that names of judges are not to be anonymized.

3 Automatization of Decisions Using AI

3.1 Towards Harmonized Rules on AI

3.1.1 On EU Level

Following the publication of the **European Strategy**[199] on artificial intelligence (AI) in 2018 and after extensive stakeholder consultation, the High-Level Expert Group on Artificial Intelligence (AI HLEG) developed Guidelines for Trustworthy AI[200] in 2019, and an Assessment List for Trustworthy AI[201] in 2020. In parallel, the first Coordinated Plan on AI[202] was published in December 2018 as a joint commitment with Member States.

The Commission's White Paper on AI,[203] adopted in February 2020, presented a clear vision for AI in Europe referring to an ecosystem of excellence and trust and setting the scene for a legislative proposal. A draft regulation laying down **harmonized rules on artificial intelligence**[204] (the AI Act) was published in April 2021, accompanied by an Impact Assessment[205] along its supporting study[206]. Again, in parallel, the Coordinated Plan on AI[207] was updated and – among others – proposed concrete actions supported by funding instruments on the coordination and resources pooling in the public sector, including judiciary.

The AI Act provides a horizontal framework and imposes regulatory burdens on AI systems that pose high risks to fundamental rights and safety. The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, law enforcement and the judiciary.

The AI Act is now being discussed by the co-legislators, namely the European Parliament and the Council (EU Member States).[208] While the Member States generally support the overall objectives of the

[199] European Commission, Communication, Artificial Intelligence for Europe, COM (2018) 237.

[200] High-Level Expert Group on Artificial Intelligence, 2019. Ethics Guidelines for Trustworthy AI.

[201] High-Level Expert Group on Artificial Intelligence, 2020. Assessment List for Trustworthy Artificial Intelligence.

[202] European Commission, Communication, Coordinated Plan on Artificial Intelligence, COM (2018) 795.

[203] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65. The White Paper is accompanied by a Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics concluding that the current product safety legislation contains a number of gaps that needed to be addressed.

[204] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206, 2021/0106(COD).

[205] European Commission, 2021. Impact Assessment of the Regulation on Artificial intelligence accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

[206] European Commission, 2021. Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe.

[207] European Commission, Communication, Fostering a European approach to Artificial Intelligence. Annex on Coordinated Plan on Artificial Intelligence 2021 Review, COM (2021) 205.

[208] European Parliament, EPRS, Artificial intelligence Act, Legislative briefing, November 2021.

proposal, questions arise as to the definition of an AI system, the scope of the draft regulation and the requirements for high-risk AI systems.

Based on the current revision of the proposal,

- the AI Act applies to – among others - Member States authorities, including judicial authorities, and Union institutions, offices, bodies, and agencies making use of AI systems, i.e., when acting as a provider or a user of an AI system
- the AI Act follows a risk-based approach and considers AI systems intended to be used by a judicial authority (or on their behalf) for interpreting facts or the law and for applying the law to a concrete set of facts, as high-risk AI systems creating adverse impact on people's safety or their fundamental rights. However, this qualification should not extend to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, or administrative tasks
- to ensure trust and consistent high level of protection of safety and fundamental rights, a range of mandatory requirements (including a conformity assessment) would apply to all high-risks systems with a view to the placing on the market or putting into service. A high-risk AI system shall be subject to strict obligations with regards to: establishing, implementing, documenting and maintaining adequate risk assessment and mitigation systems; adopting appropriate data governance and management practices to ensure high quality of the datasets feeding the system to minimise risks and discriminatory outcomes; logging of activity to ensure traceability of results; drawing up detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance; and ensuring transparency and providing clear and adequate information to the users, appropriate human oversight measures to minimise risk, and high level of robustness, security and accuracy.

Ahead of the proposal, the EU's co-legislators have considered various aspects of the potential legal framework. In October 2020, the European Parliament adopted resolutions with recommendations to the European Commission on a framework of ethical aspects of AI, robotics, and related technologies,[209] and a civil liability regime for AI,[210] followed by several other documents in a variety of AI sub-domains of application. In October 2021, European Parliament adopted a resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters,[211] based

[209] European Parliament, Legislative Observatory, Framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012 (INL).

[210] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014 (INL).

[211] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016 (INL).

on a report[212] prepared by the Committee on Civil Liberties, Justice and Home Affairs. The resolution – among others:

- considers the deployment of AI in the field of the judiciary should not be seen as a mere technical feasibility, but rather a political decision concerning the design and the objectives of criminal justice systems, whereas modern criminal law is based on the idea that authorities react to an offence after it has been committed, without assuming that all people are dangerous and need to be constantly monitored to prevent potential wrongdoing
- reminds that AI tools and applications are used by the judiciary in several countries worldwide, including to support decisions on pre-trial detention, in sentencing, calculating probabilities for reoffending and in determining probation, online dispute resolution, case law management and the provision of facilitated access to the law, whereas this has led to distorted and diminished chances for people of colour and other minorities, while at present in the EU, except for some Member States, the use of AI tools and applications is limited mainly to civil matters
- considers that any AI tools either developed or used by the judiciary should, as a minimum, be safe, robust, secure, and fit for purpose, and respect the principles of fairness, data minimisation, accountability, transparency, non-discrimination, and explainability
- considers that AI tools' development, deployment and use should be subject to risk assessment, strict necessity and proportionality testing, safeguards need to be proportionate to the identified risks, and trust among citizens in the use of AI developed, deployed and used in the EU is conditional upon the full fulfilment of these criteria
- acknowledges the positive contribution of certain types of AI applications to the work of judicial authorities across the Union highlighting, as an example, the enhanced case law management achieved by tools allowing for additional search options, considering a range of other potential uses for AI for the judiciary which could be explored while taking into consideration the five principles of the Ethical Charter on the use of artificial intelligence in judicial systems and their environment,[213] and paying particular attention to the "uses to be considered with the most extreme reservation", identified by the CEPEJ (e.g., use of algorithms in criminal matters in order to profile individuals, establishing quantity-based norm, etc.)
- stresses the potential for bias and discrimination arising from the use of AI applications such as machine learning, including the algorithms on which such applications are based; notes that biases can be inherent in underlying datasets, especially when historical data is being used, introduced by the developers of the algorithms, or generated when the systems are implemented in real world settings; and points out that the results provided by AI applications are necessarily

[212] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016 (INL).

[213] European Commission for the Efficiency of Justice (CEPEJ), 2018. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. The scope of the Charter is discussed further in the text.

influenced by the quality of the data used, and that such inherent biases are inclined to gradually increase and thereby perpetuate and amplify existing discrimination

- highlights the power asymmetry between those who employ AI technologies and those who are subject to them; stresses that it is imperative that use of AI tools by judicial authorities does not become a factor of inequality, social fracture or exclusion; and underlines the impact of the use of AI tools on the defence rights of suspects, the difficulty in obtaining meaningful information on their functioning and the consequent difficulty in challenging their results in court, in particular by individuals under investigation
- takes note of the risks related in particular to data leaks, data security breaches and unauthorised access to personal data and other information related to, for example, criminal investigations or court cases that is processed by AI systems; underlines that security and safety aspects of AI systems used in law enforcement and by the judiciary need to be considered carefully and be sufficiently robust and resilient to prevent the potentially catastrophic consequences of malicious attacks on AI systems; and stresses the importance of security by design, as well as specific human oversight before operating certain critical applications and therefore calls for law enforcement and judicial authorities only to use AI applications that adhere to the privacy and data protection by design principle in order to avoid function creep, and
- underlines that in judicial context, the decision giving legal or similar effect always needs to be taken by a human, who can be held accountable for the decisions made; considers that those subject to AI-powered systems must have recourse to remedy; and recalls that, under EU law, a person has the right not to be subjected to a decision which produces legal effects concerning them or significantly affects them and is based solely on automated data processing;
- underlines further that automated individual decision-making must not be based on special categories of personal data, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place; and stresses that EU law prohibits profiling that results in discrimination against natural persons on the basis of special categories of personal data;
- highlights that decisions in the field of law enforcement are almost always decisions that have a legal effect on the person concerned, owing to the executive nature of law enforcement authorities and their actions; notes that the use of AI may influence human decisions and have an impact on all phases of criminal procedures; takes the view that authorities making use of AI systems need to uphold extremely high legal standards and ensure human intervention, especially when analysing data deriving from such systems; requires therefore the sovereign discretion of judges and decision-making on a case-by-case basis to be upheld; and calls for a ban on the use of AI and related technologies for proposing judicial decisions.

In addition, the Council of the EU adopted Conclusions on shaping Europe's digital future[214] and on seizing the opportunities of digitalisation for access to justice, which included a dedicated section on deploying AI systems in the justice sector.[215] The Council, among others:

- underlines that the use of artificial intelligence tools must not interfere with the decision-making power of the judges or judicial independence, as a court decision must always be made by a human being and cannot be delegated to an artificial intelligence tool;
- affirms the need to explore and to decide on mandatory legal requirements to be set for the design, development, deployment, use and evaluation of artificial intelligence systems in the justice sector to effectively address the potential risks to fundamental rights – such rules could include a prohibition of automation that would make judicial decision-making opaque, appropriate levels of transparency, comprehensibility, verifiability, robustness, accuracy, security, accountability, as well as requirements to prevent discriminatory effects;
- underlines that artificial intelligence systems in the justice sector, especially those involved in judicial proceedings, should be subject to an ex-ante assessment procedure regarding inter alia the reliability, comprehensibility, robustness, and security of the system.

It is also worth mentioning that in 2020, a European strategy for data was adopted.[216] Among others, the European Commission aims at creating a common European data space for public administrations, where actions will focus on law and public procurement data and other areas of public interest such as data use for improving law enforcement in line with EU law. Seamless access to and easy re-use of EU and Member State legislation, case law as well as information on e-justice services is seen as critical not only for the effective application of EU law but also enables innovative "legal tech" applications supporting practitioners (judges, public officials, corporate counsel, and lawyers in private practice).

3.1.2 On International Level

Other international actors are also active in regulating AI. In 2019, the Council of Europe's Committee of Ministers established the ad hoc Committee on Artificial Intelligence (CAHAI)[217] to examine the feasibility and potential elements based on broad multi-stakeholder consultations, of a legal framework for the development, design, and application of AI, based on Council of Europe's standards on human rights, democracy, and the rule of law. In 2020, the Committee of Ministers of the Council of Europe adopted recommendations on the human rights impact of algorithmic systems[218] and a resolution on

[214] Council of the European Union, 2020. Shaping Europe's Digital Future – Council Conclusions, 9 June 2020.

[215] Council of the European Union, 2020. Council Conclusions "Access to Justice – Seizing the Opportunities of Digitalisation", 13 October 2020.

[216] European Commission, Communication, A European strategy for data, COM (2020) 66.

[217] See the dedicated CAHAI website.

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

the role of the AI in policing and criminal justice systems[219]. At the beginning of December 2021, the CAHAI held its 6th and final plenary meeting adopting "Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law".[220] The document contains an outline of the legal and other elements which in the view of the CAHAI could be included in legally binding or non-legally binding instruments that will make up an appropriate legal framework on AI of the Council of Europe. Towards the development of this document, the CAHAI adopted a feasibility study on a legal framework on AI design, development and application based on Council of Europe standards,[221] and published a collection of contributions presenting the global perspectives on the development of a legal framework on AI systems.[222]

The Organisation for Economic Cooperation and Development (OECD) has adopted value-based AI principles in May 2019, promoting innovative and trustworthy use of AI with respect to human rights and democratic values. OECD has also developed specific recommendation for policy makers with regards to investing in AI research and development, fostering a digital ecosystem, providing an enabling policy environment for AI, etc.[223] An AI policy observatory was set up as a one-stop-shop for data and multi-disciplinary analysis on artificial intelligence.[224]

Furthermore, at global level, on 24 November 2021 UNESCO adopted a comprehensive global standard-setting instrument to provide AI with a strong ethical basis. It not only protects but also promotes human rights and human dignity and is an ethical guiding compass and a global normative framework allowing to build strong respect for the rule of law in the digital world.[225]

These are selected examples of the wide range of legal and policy initiatives, be they actual (draft) legislation, soft-law, guidelines, and recommendations on the use of AI, or reports with recommendations for law and policy, aiming to contribute to standard setting in AI. Although the European Union Agency for Fundamental Rights (FRA) has tried to put together a list of initiatives linked to AI policymaking[226], due to the large number of such documents in recent years, the Agency acknowledged that maintaining an exhaustive list is not possible. However, it is worth noting that a **fundamental rights-centred approach to AI** is underpinned by all strategic and legislative documents, where the responsibility for respecting, protecting, and fulfilling rights rests with the State. This should

[219] Council of Europe, "Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems' Resolution (RES 2342), October 2020.

[220] The document "Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law" is to be submitted to the Committee of Ministers of the Council of Europe for further consideration.

[221] Council of Europe, 2020. Feasibility study on a legal framework on AI design, development and application based on Council of Europe standards, CAHAI (2020) 23. Supported by Artificial Intelligence, Human Rights, Democracy and the Rule of Law: a Primer, prepared by the Alan Turing Institute.

[222] Council of Europe, 2020. Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law, DGI (2020) 16.

[223] See the dedicated OECD website on AI principles and recommendations.

[224] See the dedicated OECD website on AI Policy Observatory.

[225] See the dedicated UNESCO website.

[226] See the dedicated FRA website on AI Policy Initiatives.

not only guarantee a high level of legal protection against possible misuse of AI systems, but also provide for a clear legal basis from which to develop AI, where reference to fundamental rights – and their application in practice – is fully embedded.[227] A dedicated report on the interlink between AI and fundamental rights was issued by FRA in December 2020.[228]

3.2 Ethics-by-design in AI

As mentioned, many of the existing AI initiatives are guided by **ethical frameworks**, which are typically voluntary. Almost all refer to general categories of ethical principles without a specific focus to a certain domain; for example, the High-Level Expert Group on Artificial Intelligence has called for public bodies to be held to the seven key requirements for Trustworthy AI when developing, procuring, or using AI.[229]

The "European Ethical Charter on the use of AI in the judicial systems and their environment" adopted by CEPEJ is the only one focused solely on judiciary.[230] It outlines five principles for the particular use of AI in the judicial domain, namely: (1) the principle of respect for fundamental rights (ensuring that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights), (2) the principle of non-discrimination (specifically preventing the development or intensification of any discrimination between individuals or groups of individuals), (3) the principle of quality and security (processing of judicial decisions and data using certified sources and intangible data with models elaborated in a multi-disciplinary manner, in a secure technological environment), (4) the principle of transparency, impartiality and fairness (making data processing methods accessible and understandable, authorise external audits), and the (5) "under user control" principle (precluding a prescriptive approach and ensuring that users are informed actors and in control of the choices made). Around these principles, the Ethical Charter explores various modalities of AI systems and their applications in judiciary, while addressing risks arising from systems of anticipation of judicial decisions in civil, administrative, and commercial matters, from risk assessment systems in criminal matters, and from the use of AI systems without appropriate safeguards in the framework of non-judicial alternative dispute resolution. Among those risks the CEPEJ notes the risks of "performative effect", of delegation of responsibility, and of lack of transparency of judicial decision-making. The Ethical Charter outlines:

- AI uses to be encouraged: case-law enhancement, access to law, creation of new strategic tools
- Possible AI uses, requiring considerable methodological precautions: help in the drawing up of scales in certain civil disputes, support for alternative dispute settlement measures in civil matters, online dispute resolution, the use of algorithms in criminal investigation to identify where criminal offences are being committed

[227] European Union Agency for Fundamental Rights, 2019. Fundamental Rights Report 2019, Luxembourg, Publications Office, Chapter 7.

[228] European Union Agency for Fundamental Rights, 2020. Getting the future right – Artificial intelligence and fundamental rights. Luxembourg, Publications Office.

[229] Namely, human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination, and fairness; environmental and societal well-being; and accountability.

[230] Although this non-binding instrument is classed as an ethical charter, to a large extent it concerns legal principles enshrined in international instruments.

- AI uses to be considered following additional scientific studies: judge profiling, anticipating court decisions
- AI uses to be considered with the most extreme reservations: use of algorithms in criminal matters to profile individuals, quantity-based norm.

The work of the CAHAI is also of particular importance in respect to the above. With regards to judiciary, focus is placed on the large-scale risk exposure in AI systems towards group discrimination, considering the difference between errors in human and machine decision making has an important consequence in terms of scale – while human error affects only individual cases, an AI system with a poor and/or bias design but being applied to a whole series of cases affect all people in the same or similar circumstances.[231] Attention is given to the important role that the natural language processing plays in AI applications for the justice sphere, considering the textual nature of legal documents; thus, requiring each jurisdiction to adopt a solution developed with a focus on its official language in mind. Implicit unexpressed reasoning in legal decisions and the presence of general clauses require relevant legal interpretation and are considered unamenable by language-based machine learning tools.[232]

Further, CAHAI calls for "a careful and more critical adoption of AI in the field of justice than in other domains" and, with regard to court decisions and alternative dispute resolutions, "a distinction between cases characterised by routinely and fact-based evaluations and cases characterised by a significant margin for legal reasoning and discretion".[233] Some AI tools facilitate content and knowledge management, organisational management, and performance measurement, and relate to applications such as contracts categorisation, detection of divergent or incompatible contractual clauses, e-discovery, drafting assistance, law provision retrieval, assisted compliance review, basic problem-solving functions based on standard questions and standardised situations (e.g. legal chatbots), etc.[234] In such cases, AI systems may affect legal practice and knowledge, but the potential adverse consequences remain limited and are mainly related to the inefficiencies or flaws of these systems. Ethical and legal issues may refer to product liability, bias and non-discrimination, transparency, principles of fair trial and equality of arms, etc.[235]

Where AI systems are designed to automate or support judicial decisions, issues become critical. Considering the distinction between codified justice and equitable justice,[236] it is concluded that AI

[231] See also the 2019 report by the Big Brother Watch group in the UK discussing the problems of the training data for predictive policing algorithms in the UK and the resulting biased and discriminatory decisions.

[232] Op. cit. Towards regulation of AI systems, DGI (2020) 16, p. 85.

[233] Op. cit. Towards regulation of AI systems, DGI (2020) 16, p. 85.

[234] See European Commission for the Efficiency of Justice (CEPEJ). 2018. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment, Appendix II.

[235] Op. cit. Towards regulation of AI systems, DGI (2020) 16, p. 85-86.

[236] Re, R.M., Solow-Niederman, A. 2019. Developing Artificially Intelligent Justice. 22 Stan. Tech. L. Rev. 252-254 ("Equitable justice entails both reflection on the values set in place by the legal system and the reasoned application of those values, in context […] Codified justice refers to the routinized application of standardized procedures to a set of facts […] In short, codified justice sees the vices of discretion, whereas equitable justice sees its virtues").

should be circumscribed for decision-making purposes to cases characterised by routine and fact-based evaluations.[237] The logic of equitable justice is more complicated than the simple outcome of individual cases; it is considered that expressed and unexpressed legal and non-legal values and considerations that characterise the reasoning of the courts are not replicable by the logic of AI. The social role courts play is also placed against the deductive and path-dependent nature of the AI tools. In specific cases, including in alternative dispute resolutions, "both the mediation between the parties' demands and the analysis of the psychological component of human actions (fault, intentionality) require emotional intelligence that AI systems do not have". The documents further explore issues such as equal treatment before the law and non-discrimination, principles of fair trial and of equality of arms, data quality, transparency, the independence of the judges, the need for human oversight, etc.[238]

The complementing report from the Alan Turing Institutes further maps how each of the principles and priorities under the European Convention of Human Rights and the European Social Charter relates to corresponding rights and obligations within the context of the rule of law:

- "Member States must ensure that AI systems used in the field of justice […] are in line with the essential requirements of the right to a fair trial. To this end, they should ensure the quality and security of judicial decisions and data, as well as the transparency, impartiality, and fairness of data processing methods. Safeguards for the accessibility and explainability of data processing methods, including the possibility of external audits, should be introduced to this end.
- Member States must ensure that effective remedies are available and that accessible redress mechanisms are put in place for individuals whose rights are violated through the development or use of AI systems in contexts relevant to the rule of law.
- Member States should provide meaningful information to individuals on the use of AI systems in the public sector whenever this can significantly impact individuals' lives. Such information must especially be provided when AI systems are used in the field of justice […], both as concerns the role of AI systems within the process, and the right to challenge the decisions informed or made thereby.
- Member States should ensure that use of AI systems does not interfere with the decision- making power of judges or judicial independence and that any judicial decision is subject to meaningful human oversight."[239]

3.3 Standardisation of AI Systems

The AI Act puts **standardisation** in a key role to provide technical solutions to providers to ensure compliance. However, the standardization of AI systems is not a matter of purely technical decision, and a series of legal and ethical decisions must be taken that require a political debate. In this, the

[237] Op. cit. Towards regulation of AI systems, DGI (2020) 16, p. 86.

[238] Op. cit. Towards regulation of AI systems, DGI (2020) 16, p. 86-87.

[239] Alan Turing Institute, 2020. Artificial Intelligence, Human Rights, Democracy and the Rule of Law: a Primer, p. 23.

European standardization process must reflect European values and fundamental rights, including consumer protection by granting European stakeholder organizations effective participation rights.

Few standards and standardisation preparatory works are in place, none of which are to be applied restrictively to judiciary. For example, the British Standard (BS) 8611:2016[240] gives guidelines for the identification of potential ethical harm arising from the growing number of robots and autonomous systems being used in everyday life. The standard also provides additional guidelines to eliminate or reduce the risks associated with these ethical hazards to an acceptable level, and covers safe design, protective measures and information for the design and application of robots.

The Institute of Electrical and Electronics Engineers (IEEE) "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems"[241] is a comprehensive report that combines a conceptual framework addressing universal human values, data agency, and technical dependability with a set of principles to guide autonomous and intelligent systems creators (designers, developers, engineers, programmers, and others) and users through a comprehensive set of recommendations. Among others, the report aims to inspire the creation of standards (IEEE P7000™ series and beyond) and associated certification programs. The IEEE P7000 series refers to the IEEE Standards Project for Model Process for Addressing Ethical Concerns During System Design for identifying and analysing potential ethical issues in a system or software program from the onset of the effort. The values-based system design methods address ethical considerations at each stage of development to help avoid negative unintended consequences while increasing innovation; and encompasses two adopted and eleven draft standards.[242] Considering their scope, only P7000 to P7003 are considered relevant to the judicial domain. The IEEE P7000™-2021 "Standard Model Process for Addressing Ethical Concerns during System Design" is already available since September 2021. Three other standards covering the topics of transparency, privacy, and algorithmic bias are still at draft stages.

Considering national approaches, "[m]any governments also implement monitoring and reward systems for compliance with principles for trustworthy AI. Malta has developed an AI certification framework, issued by the Malta Digital Innovation Authority (MDIA). It serves as valuable recognition in the marketplace that the AI systems of successful applicants have been developed in an ethical, transparent and socially responsible manner […]. Similar quality seals or labels - acting as hallmarks for a responsible approach in AI - have been adopted in other countries such as Denmark and Germany. The Czech Republic, Italy, Lithuania, and Spain are considering developing them as well. Similarly, the AI registers set up by the cities of Amsterdam and Helsinki […] aim to ensure a secure, responsible and

[240] British Standard (BS) 8611:2016 "Robots and Robotic Devices: Guide to the Ethical Design and Application of Robots and Robotic Systems".

[241] See the dedicated website of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems.

[242] See https://ethicsinaction.ieee.org/p7000/.

transparent use of AI algorithms."[243] Unfortunately, none of the schemas considers specifically the issues of the judicial domain.

In December 2020, CEPEJ adopted a feasibility study on the possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary.[244] Closely following the work of the CAHAI, the document also distinguishes between the categories of uses of AI in judiciary and focuses on predictive justice as the category with strongest ramifications for fundamental rights and freedoms. The diversity of judicial systems, judicial professionals (namely, judges[245]) and legal domains is also taken into consideration, alongside the typology of AI systems and the taxonomy of socio-technical aspects of AI risks. The document explores the typology and challenges of certification and labels and the potential objectives of CEPEJ certification; sets out the issues linked to certification deployment, in terms of certification authorities, governance structure, and the risks and opportunities entailed in such certification by the CEPEJ and the issues of responsibilities linked to certification deployment; and concludes with a review of the AI Act in light of the study and a potential schedule and roadmap to be followed.

Although not directly linked to classic standardisation process, it is worth mentioning an initiative by the European Law Institute to deliver Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration.[246] Alternative rules are also discussed and proposed to facilitate the adaptation of rules to different levels of ambition. The draft rules are currently under internal evaluation and expected to be soon finalized.[247] This approach could also be adopted by the judiciary, where the national judicial management body allows for decentralised management of IT projects across judicial authorities.

3.4 Regulatory Sandboxes

The AI Act encourages Member States to establish artificial intelligence **testing initiatives** such as regulatory sandboxes, test beds, laboratories, innovation spaces or experimentation programmes, to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service. Some Member States are already making significant progress in this area. For example, to systematically establish regulatory sandboxes as an instrument of economic and innovation policy the German Federal Ministry for Economic Affairs

[243] Van Roy, V., Rossetti, F., Perset, K., Galindo-Romero, L. (2021) AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition, p. 15. EUR 30745 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-39081-7, doi:10.2760/069178, JRC122684.

[244] European Commission for the Efficiency of Justice (CEPEJ), 2020. Possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary: Feasibility Study. See also Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Council of Europe study, DGI (2017) 12.

[245] For example, in France decisions are handed down, depending on the case, by courts made up solely of professional judges, by lay auxiliary judges, by trade union representatives, or by juries.

[246] See the dedicated ELI website on the model rules.

[247] See ELI website, "AI and Public Administration Project Team Making Final Adjustments to their Model Rules", 24 November 2021.

and Energy adopted a Regulatory Sandboxes Strategy in December 2018. Later, the same ministry published a handbook for regulatory sandboxes[248] to improve the degree of expertise relating to regulatory sandboxes on both national and EU levels. While the handbook heavily explores projects in e-government, the e-justice domain is not particularly considered.

In its November 2020 conclusions on regulatory sandboxes and experimental clauses,[249] the Council of the EU already highlighted that "flexibility and experimentation can be important elements for an agile, innovation-friendly, future-proof, evidence-based and resilient regulatory framework which fosters competitiveness, growth, sustainability, regulatory learning as well as European technological sovereignty and leadership, and which helps to master systemic shocks and disruptive as well as long-term future challenges", and called on the Commission to "organise, in cooperation with Member States, an exchange of information and good practices regarding regulatory sandboxes between Member States and itself in order to: a) establish an overview of the state of play regarding the use of regulatory sandboxes in the EU; b) identify experiences regarding the legal basis, implementation and evaluation of regulatory sandboxes; c) analyse how learning from regulatory sandboxes at national level can contribute to evidence-based policy making at EU-level."

In April 2021, the Commission presented its first findings on experimental clauses in the EU legislation[250] before proceeding with gathering more information on the state of play of regulatory sandboxes in the EU.[251] As a steppingstone, a variety of practices mostly from the financial sector were considered.[252] An overview of EU Member States responses was presented during the meeting of the Working Party on Competitiveness and Growth (Better Regulation) that took place on 1 December 2021.[253] This is expected to be made publicly available soon.

In the judicial domain, the regulatory sandboxes could be used to establish a controlled experimentation and testing environment in the development and testing phases with a view to ensure compliance of the AI systems with the AI Act and other relevant Union and Member States legislation; to enhance legal certainty; and to ensure the competent authorities' oversight and understanding of the emerging risks and the impact of AI uses. Further, judiciary could adopt novel regulatory practices to respond in a more agile way to innovation and disruption, better grasping the opportunities and

[248] German Federal Ministry for Economic Affairs and Energy, 2019. Making space for innovation. The handbook on regulatory sandboxes.

[249] Council of the European Union, 2020. Council Conclusions on regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, 16.11.2020.

[250] Council of the European Union, 28.04.2021, WK 5521/2021 INIT.

[251] Council of the European Union, 05.07.2021, WK 10338/2021 INIT.

[252] Parenti, R., Regulatory Sandboxes and Innovation Hubs for FinTech, Study for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, p. 21. ("Globally, the UK FCA spearheaded this practice by establishing its regulatory sandbox in 2016, and a number of other jurisdictions followed suit. Currently, six Member States (DK, HU, LT, LV, NL, MT), as well as Norway among the EFTA countries, already have an operational one. In addition, other six Member States (AT, EE, EL, ES, IT, PL) are in an advanced preparatory stage of establishing a sandbox. A few thereof (EL, EE and PL) are being developed with support under the Structural Reform Support Programme (SRSP) Regulation, implemented by the EBRD with assistance by the Commission services (DG REFORM). Two more Member States have either announced intentions to set up a sandbox (BG) or are currently analysing the benefits and possible implementation thereof (SK).")

[253] Council of the European Union, 24.11.2021, CM 5554/2021 INIT.

mitigate the risks they enable. However, techniques such as anticipatory regulation[254], outcome-focused regulation,[255,256] experimental regulation,[257] or data-driven regulation,[258] are still not supported by significant evidence on their long-term efficiency and effectiveness compared to the exciting pool of regulatory practices; thus, their usage and impact should be carefully monitored and evaluated if implemented.

Research shows that several US[259] and Canadian[260] states have legal regulatory sandbox proposals under consideration; however, no relevant European examples were found.[261] For reference, Germany's AI strategy plans the establishment of AI regulatory sandboxes and testbeds, such as the "Digital Motorway testbed A9" (administrated by the Federal Ministry of Transport and Digital Infrastructure). Similarly, the Italian Government put in place regulatory sandboxes through the

[254] The concept of anticipatory regulation refers to identification of changes beyond the domain in question over a given period and consideration of the implications of these changes (jointly or individually) for the regulator's current and future approaches, i.e., with regards to the impact of technological innovation. Examples of successful practice can be given in: Sweden, where in 2018 the Swedish Government set up a Committee on Technological Innovation and Ethics to identify conflicting goals, regulatory challenges, and barriers to the responsible use of new technologies (such as AI, machine learning, etc.); Japan, where the Japanese Ministry of Land, Infrastructure, Transport and Tourism has adopted agile regulation approach to explore the potential of autonomous vehicles by using a system of exemptions, to permit the trialling of autonomous vehicles that do not meet ordinary regulatory requirements, co-developing voluntary technical requirements with industry for the training of the autonomous vehicles, adapting technical requirements based on data from trials and with a focus on international harmonization, and finalizing requirements once the technology is sufficiently distributed in the market; etc.

[255] Also known as goal-based regulation, it places a focus on the achievement of "real-world" outcomes for end-users and the environment and defines high-level goals that stakeholders' actions must achieve using their own judgement (by employing or combining such techniques as experimentation clauses and regulatory guidance). It is distinct from prescriptive rules-based regulation, which defines in advance precisely what actions stakeholders must or must not do. See also United Kingdom Government, Department for Business, Energy & Industrial Strategy (BEIS), "Goals-based and rules-based approaches to regulation", BEIS Research Paper No. 8, May 2018. Non-binding instruments (soft law), such as regulatory guidance, code of practices, and voluntary standards may complement such efforts to reduce business uncertainty.

[256] Examples on applying performance-based regulations can be given with the efforts of Rwanda on drone technology, the introduction of the "right to innovate" in Italy and Japan, introduction of experimental clauses in energy, media, and transport in Germany, etc.

[257] Experimental regulation refers to a process of learning and adaptation, where regulators engage with businesses on ideas, products, and business models to learn how both parties need to adapt to enabled innovative products and services to be brought to market efficiently.

[258] This concept refers to introducing rules as machine-readable code and is also known as machine-consumable regulation. Data-driven technologies enable a new approach to regulation, in which interventions may be finely targeted, outcomes may be monitored in real time and rules may be evaluated and updated at pace. As systems mature, regulators could use the data gathered to help model the effects of future changes to their code, and businesses could execute changes to their systems much more rapidly, enabling a much more agile governance system. See also World Economic Forum, "Agile Regulation for the Fourth Industrial Revolution A Toolkit for Regulators", December 2020, p. 27-31. Examples of such practices can be found in New Zealand, Australia, and Canada that are making efforts to develop machine-consumable regulation.

[259] For example, Utah, Arizona, California, etc. See the 2020 work of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC), titled Fostering Innovation in Legal Services: Testing Legal Regulatory Changes in a Protected "Sandbox".

[260] Namely British Columbia and Ontario.

[261] Van Roy, V., Rossetti, F., Perset, K., Galindo-Romero, L. (2021) AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition, p. 16. EUR 30745 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-39081-7, doi:10.2760/069178, JRC122684.

"Sperimentazione Italia" initiative to facilitate controlled experiments with innovative products, including AI. Neither, though, aim for judicial advances in the field.

Although not directly linked to the topic, it is worth mentioning a study by the Joint Research Centre (JRC), the European Commission's science and knowledge service, that could support the adaptation of judicial research to a technology that is ready to use in real-world environments.[262] This document describes an example-based methodology to categorise and assess several AI technologies, by mapping them onto Technology Readiness Levels (TRL) (e.g., maturity and availability levels). Some of the exemplary technologies are considered relevant to judicial purposes, such as machine translation, speech recognition, text recognition, negotiation agents, and virtual assistants.

Considering this reference, another interesting JRC report that could support the judicial domain explores the use and impact of AI in public services in the EU.[263] This report presents the results of the first exploratory mapping of the use of AI in public services in the EU, which contributes to landscaping the current state of the art in the field, and provides an overview of Member States' efforts to adopt AI-enabled innovations in their government operations, including audio processing, intelligent digital assistants and chatbots (being the most heavily exploited sub-category), text mining and speech analytics, predictive analytics, simulation and data visualisation, etc.

Related to the encoding of legislation, it is also worthwhile mentioning that, in the future, software aimed at processing legislation may source from many interconnected resources, provided by a heterogeneous group of organisations, each responsible for its own domain. It would be helpful to resolve missing domain knowledge through semantic reasoning and the interconnection of domains. Therefore, research shows that it is important to follow up on evolutions in data processing in communities that have a strong affinity with the legal and the compliance domain, such as: standardisation (machine-readable and executable compliance[264]), finances (implementing regulatory concepts and reporting obligations by assisted machine learning[265]), e-Government (structured representations of local decision making[266]), and e-Tendering (compliance checking[267]).

3.5 National Strategic and Regulatory Efforts

Reviewing the **AI strategies across EU and EEA states**, research shows that Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Latvia, Lithuania, Luxembourg,

[262] Martínez-Plumed, F., Gómez, E., Hernández-Orallo, J., AI Watch: Assessing Technology Readiness Levels for Artificial Intelligence, EUR 30401 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-22987-2, doi:10.2760/15025, JRC122014.

[263] Misuraca, G., and van Noordt, C., Overview of the use and impact of AI in public services in the EU, EUR 30255 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19540-5, doi:10.2760/039619, JRC120399.

[264] See, for example, the description of the "Standards for the Future" project in CEN's (the European Committee for Standardisation) and CENELEC's (the European Committee for Electrotechnical Standardisation) Work Programme 2021, p. 109.

[265] See, for example, DG FISMA's Report on "Implementing dictionaries of regulatory concepts and reporting obligations by assisted machine learning" from October 2021.

[266] See, for example, the "Lokale besluiten als gelinkte open data" project ("Local governmental decisions as linked open data"; in Dutch).

[267] See, for example, the work done at the eProcurement joinup.

Malta, the Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, and Sweden have published national AI strategies.[268]

- The Austrian Government has been very active in shaping policy initiatives, with recommendations on robotics and AI, covering policy areas related to smart governance, smart innovation, and smart regulations. The Austrian Federal Ministry of Justice explicitly highlights the use of AI for evaluating judicial proceedings, as mentioned in its national e-justice strategy.[269]
- The Finnish Ministries of Justice and Finance are currently examining national regulation of automated decision-making. The impact assessment of algorithmic decision making is presented in a policy report "Algorithm as a decision maker?: Opportunities and challenges for the use of artificial intelligence in the national regulatory environment" that was commissioned by the Finnish Government and released in 2019.[270]
- Hungarian strategy calls for the development of sector-specific regulatory frameworks, ensuring that the regulatory needs for AI development are adapted to the relevant industry areas. In a collaboration between the Ministry of Justice, the Ministry for Innovation and Technology, AI Innovation Hub and the Central Statistical Office, an ethical framework – an AI Code of Conduct – is under development.[271]
- The Latvian strategy identifies priority sectors with a high potential for AI applications in the country, including the justice domain with a focus on AI as support for decision making and drafting legislation.[272]

Furthermore, the Swiss government seeks advancements in seventeen thematic fields, including with regards to AI in justice, while trying to adopt a technology-neutral policy to avoid the promotion of specific technologies and of technology-specific regulations as far as possible. The establishment of the legal basis is currently ensured by a wide range of institutions, while the Federal Department of Foreign Affairs specifically focuses on policies to further develop the general legal framework on AI by examining the emergence of AI-specific international law and its impact on Switzerland, following-up developments with regard to the visibility of AI systems in interaction with consumers, and monitoring developments in AI-based decision-making in the justice system (predictive justice).[273] The judiciary may in principle use AI as a tool, even if this concerns the legal position of persons, provided that the necessary legal basis exists.

[268] Overview can be found at AI Watch. Further, EC-OECD database of national AI policies contains national AI strategies and AI-related policy initiatives from over 60 countries.

[269] Available here.

[270] Available here.

[271] Available here.

[272] Available here.

[273] Available here.

States are also seeking to develop **sector-specific regulations** for well-defined AI fields that are not yet (sufficiently) covered by existing EU legislation, such as automated driving and associated technologies on public roads (e.g., Austria, Belgium, Czech Republic Germany, Lithuania, and Spain), data governance and/or automated decision making in healthcare (e.g., Norway), data governance enhancements in privacy (e.g., Slovenia), etc. While the adopted approaches might be of interest for the purpose of using AI in the judicial domain, several other initiatives are highly contextually linked as well.

- The Dutch Government has already implemented the Law Enforcement Directive[274] in its national legislation, embedding provisions on automated decision making for law enforcement.
- Finland and Portugal are in the process of drafting national legislation for automated decision-making to determine – among others – liability issues.
- France is working on introducing AI in the field of justice by adopting a decree named "Data Just"[275] of 27 March 2020. Its purpose is to create an AI aimed at carrying out evaluations of public policies in the field of both civil and administrative liability, developing an indicative reference framework for personal injury compensation for professionals and individuals, informing the parties (victims, insurers) in order to encourage settlements, and providing a benchmark for judges in the field of personal injury compensation. The French Data Protection Authority has asked the Ministry of Justice, among other things, to provide within a year from the end of the development phase (undergoing), a detailed description of the algorithm, the methods used, the biases of the algorithm identified, and the corrections envisaged/applied.[276]

An interesting example beyond European borders can be given with Canada, where the Government launched a Directive on Automated Decision Making[277], purported to use AI to assist the government in replacing mundane administrative tasks within all its branches. The Directive applies only to systems that provide external services as defined in their Policy on Service and Digital[278] (any system, tool, or statistical model in production used to recommend or make an administrative decision about a client). The Directive prescribes such systems to go through algorithmic impact assessment[279] and cover the requirements for transparency, quality assurance, recourse, and reporting.

[274] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

[275] See legifrance.gouv.fr.

[276] See legifrance.gouv.fr.

[277] See Government of Canada's website on the Directive on Automated Decision Making.

[278] See Government of Canada's website on the Policy on Service and Digital.

[279] See Government of Canada's website on the Algorithmic Impact Assessment Tool.

3.6 National Initiatives and Projects

3.6.1 EC Study on the Use of Innovative Technologies in the Justice Field

With regards to actual deployment of AI tools in judiciary, a 2020 Commission study has shown that while Member States are willing to adopt AI, the progress is still slow and varies greatly between and within states.[280] It should be noted that the study was not centralised. With regards to both replies on strategy, legislation and projects more than one institution per state was inquired, which affected the results towards disproportionality and over-/underrepresentation. For example, Italy provided 35 replies, Sweden - 13, Portugal – 7, the Netherlands – 6, and Denmark – 5, in comparison to all other countries providing up to three replies.

Replies on strategy and legislation are collected from public authorities and the judiciary; however, it should be noted that the judicial respondents represent only 29% of all surveyed participants.

- 51% of the respondents (a total of 69 replies received) have pointed out that there were in place strategies/policies governing the use of innovative technologies in the justice field, while 14% of the respondents selected "Other".[281]. Assessing the Member States, positive replies have been given for Austria, Czech Republic, Denmark, France, Italy, the Netherlands, and Spain.
- Only 16% of the respondents (a total of 57 replies received) have confirmed that there was national legislation in force applicable to the use of AI in the justice field, while 23% of the respondents selected "Other".[282] Assessing the Member States, positive replies have been given for Germany, Italy, the Netherlands, and Sweden.

When asked whether the respondents' organisations are currently involved in projects using AI in the justice field, a total of 52 replies from stakeholders have been received, where:

- 13 (or 25% of the 52 replies) selected "None",
- 29 (or 55% of the 52 replies) selected "1-3 projects",
- 5 (or 10% of the 52 replies) indicated "4-5 projects", and
- 5 (or 10% of the 52 replies) selected "More than 5 projects".

A total of 75 AI project were presented;[283] with most notable number of projects coming from Italy (33), Sweden (13), Portugal (7), the Netherlands (6) and Denmark (5). An additional list of initiatives and ideas for future implementation of AI by the Member States' authorities or judiciary have been discussed with the stakeholders during the interview consultations and is presented below.[284]

[280] European Commission, 2020. Study on the use of innovative technologies in the justice field. Data presented reflects the situation as of 7 April 2020.

[281] No elaboration on this option is provided.

[282] No elaboration on this option is provided.

[283] European Commission, 2020. Study on the use of innovative technologies in the justice field, pp. 111-142.

[284] Ibid, pp. 143-147.

The study groups the business problems tackled during the implementation of the projects carried out by public authorities and the judiciary in the Member States, and by legal professional organisations, in eight categories, namely: processing high volume of data;[285] processing high volume of video, audio, and images;[286] linking information across different sources;[287] access to justice/public services;[288] data protection compliance;[289] preparing high volume of data;[290] administrative/facilities management;[291] and lack of authenticity and traceability.[292] Then, the study[293] maps the business problem categories to business solutions[294] that the projects using AI aim to achieve:[295]

- Anonymisation and pseudonymisation (used in 12 projects) – using AI technology to automate the manual identification and removal of personal data (and/or other sensitive data) as a solution to business problems in the categories of preparing or processing high volumes of data and data protection compliance. Such projects have been identified in Austria (1), Croatia (1), Czech Republic (1), Denmark (2), Finland (1), France (1), Germany (1), Italy (1), Luxembourg (1), Spain (1), and Sweden (1). An example for such project is the one put in place by the French Supreme Court on AI-driven pseudonymization of court decisions.[296] The goal of the project is to provide an automated and faster pseudonymisation of French court decisions. The tool solves the business problem with more than 70% accuracy and increased productivity (with AI automating

[285] The issue of processing high volumes of structured and unstructured data and documents manually or with simple digital tools, to make an analysis based on the content for tasks such as: finding relevant information for the case, deducting patterns, searching for specific words or cases, classification, and categorisation, etc.

[286] The issue of processing a high volume of video files, audio files and/or images to make an analysis of the content for tasks such as: identification of persons/victims, or monitoring of behaviour, detecting illegal activities, transcription to text, etc.

[287] The issues of looking for, extracting, and analysing information from multiple sources (such as different databases, registers, systems, etc.), usually because they are not centralised, or connected, and there is no common interface or access point.

[288] The issue of not making judicial information or public services available to the citizens/the public in a user-friendly and easily accessible way. It includes access to case law, case information, legislation, treatment of citizens' questions, navigation through administrative procedures, etc.

[289] The issue of making documents (usually court judgments and decisions) compliant with the personal data protection legislation with the aim of making those documents publicly available.

[290] The issue of treating (high volumes of) data manually, or with simple digital tools to obtain a final output, e.g., in preparation of court hearings and in conducting court administration tasks, and/or other judicial tasks. This involves tasks such as: translation of documents, typing of protocols in court hearings or interviews, preparation of contracts, judicial decisions and anonymised versions thereof, manually signing documents, etc.

[291] The issue of managing the court administration processes performed by the judicial personnel (clerks, judges, lawyers, etc.), with tasks such as planning of the agendas, court hearings, booking and allocation of court rooms and infrastructure, organising interviews and doing the facility management.

[292] The issue of having an insufficient level of traceability regarding actions to be taken by different actors related to data and documents during their process flows (e.g., invoices, diplomas, proxies etc.), so that the information can be stored and/or transferred with a sufficient level of authenticity, trust, and integrity.

[293] European Commission, 2020. Study on the use of innovative technologies in the justice field, pp. 198-218. Overview of Member States' authorities' projects per business problem and solution category is presented.

[294] One business solution may solve more than one business problem as per the identified business problem categories.

[295] European Commission, 2020. Study on the use of innovative technologies in the justice field, pp. 367-442. Full list of AI Projects is presented in Annex II "Explored projects and use cases of the Member States' authorities".

[296] Ibid, pp. 408-409.

low-value, routine activities), ensuring consistency in decisions (e.g., judgements) and repeatability/reproducibility (e.g., judgements) for verification purposes. It is considered the tool meets the expectations; and it is expected that with the tool in place, more than 4 million court sentences a year will be published in line with the law pertaining to open data of sentences.[297]

- Digital assistance (used in 4 projects) – using AI technology, such as chatbots, to improve citizens' access to information and navigate them through administrative processes; thus, ensuring access to justice/public services. Such projects have been identified in Austria (1), Finland (1), Portugal (1), and Sweden (1). An example in this regard is the Portuguese project IReNe[298] providing a web personal assistant, implemented by the national Institute of Registries and Notaries. The project's main objectives refer to improving the quality of services for citizens, more efficiently managing the organisation, and improving the organisation's relationship with customers and the quality of customer services provided. To this end, the tool supports answering frequently asked questions (FAQs) based on a knowledge base managed by the Institute, interpreting the citizen's intention to renew an ID card and assessing the citizen's particular situation, and suggesting the most suitable method of renewing the card: online, face-to-face or by appointment. The smart channel also allows the citizen to schedule online an appointment if this is the most suitable option. In the case of spontaneous services, it offers average waiting times and is integrated with Google Maps so that, depending on the route and means of travel, one can choose the most appropriate counter.
- Facial and/or object recognition (used in 5 projects) – typically using AI technology to detect, identify and verify a person or an object from a digital image or video footage based on specific facial or other features; such solutions are used in criminal justice to improve victim identification from pictorial material or detect abnormal behaviour of inmates in prisons. Such projects have been identified in Austria (1), Denmark (1), Germany (1), and Ireland (2). An example in this sense is a project from Germany on fighting child pornography[299], managed by the Central Cybercrime Department to the Ministry of Justice North-Rhine-Westphalia. The main objectives are to improve the efficiency of justice by achieving a faster time-to-trial and increasing the number of rulings in less time. The current stage of the project is the training of the AI solution and testing the solution on an actual case, to be followed by potential development in a production environment (to be reviewed by the responsible competent authorities).
- Predictive analytics or predictive justice (used in 5 projects) – using AI technology to analyse current and historical facts to make predictions about the future or and/or identify risks and opportunities; in the justice field, such solutions are typically used to help the judiciary in the decision-making process. Such projects have been identified in France (1), Italy (2), Portugal (1),

[297] Further information on open data in France is provided in Section 2.2.3 of the present report.

[298] Ibid, pp. 382-383.

[299] Ibid, pp. 409-410.

and Sweden (2).[300] An example of project is the one implemented by the Court of Genoa on predictive algorithms for judicial decisions based on semantic analysis of previous decisions.[301] The project is developed jointly with the Sant'Anna School of Advanced Studies in Pisa and CNR, authorised by the Ministry of Justice of Italy. The primary objective is to build analytical and predictive algorithms for jurisprudence along with ensuring the necessary knowledge of the algorithm.

- Process automation (used in 32 projects) – using AI technology and (robot) process automation, to automate processes such as organisation, planning and facilities management, prioritisation, categorisation and allocation of documents and tasks; in the justice field, process automation is used to improve efficiency by automating manual and repetitive tasks such as analysing case-related information (e.g., data collected from house searches), payment of fines by citizens, etc. Such projects have been identified in Austria (2), Denmark (3), Finland (1), Germany (3), Italy (9), Lithuania (1), the Netherlands (2), Portugal (4), Slovenia (2), Spain (1), and Sweden (4).[302]
- Search optimisation (used in 10 projects) – using AI technology to expedite and facilitate searches in relevant case law, registers, and digital libraries, usually creating semantic links and possibilities for document annotation. Such projects have been identified in Austria (1), Italy (1), Malta (2), the Netherlands (1), Portugal (1), Spain (3), and Sweden (1). An example in this regard is a project from the Dutch Ministry of Justice and Security delivering a Jurisprudence-robot[303]. To ensure district attorneys can quickly obtain relevant jurisprudence and other necessary information from underlying data, the tool makes use of automated business processes (legal workflow automation), improve efficiency and accuracy, and provide better insight on the available data. The tool is still under development.
- Speech/text-to-text/speech solutions (used in 9 projects) – using AI technology, such as voice recognition and machine translation; in the justice field, such solutions are used to modernise court rooms and facilitate court hearings by replacing the manual typing of court minutes and other documents or for translations from foreign languages. Such projects have been identified in Croatia (1), Estonia (1), Germany (2), Hungary (1), Latvia (1), Spain (1), and Sweden (2). Some

[300] Estonia also embraces AI as a key solution to predict results of processes and discover new patterns to tackle the growing complexity of court cases from the local to the European Union level. See e-estonia, 2020, on "Artificial intelligence as the new reality of e-justice". See also Niiler E., 2019, "Can AI Be a Fair Judge in Court? Estonia Thinks So", Wired, on Estonia piloting a program in which small scale civil suits are decided by an algorithm.

[301] European Commission, 2020. Study on the use of innovative technologies in the justice field, pp. 418-419.

[302] Latvia stated that it was exploring the possibilities of machine learning for the administration of justice. The main purpose would be to process court statistics to draw up provisional estimates of human and financial resources to be allocated. See European Commission for the Efficiency of Justice (CEPEJ). 2018. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment, p. 17.

[303] European Commission, 2020. Study on the use of innovative technologies in the justice field, pp. 381-382.

good examples are the Swedish projects on speech-to-text and text-to-text translation implemented by the National Courts Administration.[304]

In addition to the projects and initiatives studied, some stakeholders shared ideas during the interviews for potential usage of AI that may be worth further exploration, and which could grow into initiatives and/or projects such as for example, the possible use of virtual assistance (chatbots), the use of data science and predictive analytics, facial recognition from surveillance cameras to increase security in the institution, the automation of case law references and "clickable citations", the graphic representations of relations between cases, a thesaurus and automated translation functionalities, single search windows for all relevant case law, legislation, and internal studies databases, etc.[305]

Further, the study acknowledges the work of the Court of Justice of the European Union that has also prepared a target architecture strategy. The latter has the main objectives to increase security, quality, and productivity using, among others, AI, exploring pilots in (re-usable) machine translation, text analysis using AI, court's documents classification, legal text automatic detection, (pseudo-)anonymisation, speech-to-text and search engines evolution, optical character recognition, data visualisation, and chatbot (in the area of end-user support or large internal public communication).[306]

In summary, research shows that AI is used or being explored in European legal systems for a variety of purposes, such as facilitating case management, access to law, supporting alternative dispute settlement measures in civil matters, online disputes, or "judge profiling". Judicial authorities are increasingly adopting AI-based applications. Of particular interest in the field of justice are the anonymisation of court decisions, speech-to-text conversion and transcription, machine translation, chatbots supporting access to justice and process automation (automation of processes such as organisation, planning and facilities management, prioritisation, categorisation and allocation of documents and tasks by robots).

3.6.2 EU-funded Projects

2019-2023 Action Plan European e-Justice[307] addressed the topic of AI for the first time, with the Justice Programme 2014-2020[308] placing funding focus on e-justice projects using AI in 2019 onwards; yet some projects on AI basics found funding even in earlier stages. Few AI-related projects have been funded to date, namely:

– "Conflict Resolution with Equitative Algorithms" (CREA), Grant Agreement 766463,[309] run by a wide European Consortium. The project aimed to introduce new mechanisms of dispute

[304] Ibid, pp. 386 and 440-441.

[305] Ibid, p. 58.

[306] Ibid, p. 48-49.

[307] European Commission, 2019-2023 Action Plan European e-Justice. OJ C 96, 13.3.2019, p. 9–32

[308] Regulation (EU) No 1382/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Justice Programme for the period 2014 to 2020. OJ L 354, 28.12.2013, p 73–83.

[309] Summary is available here. See also dedicated project website. Project is running 2017-2019.

resolution as a helping tool in legal procedures for lawyers, mediators, and judges with the objective to reach an agreement between the parties; in some situations, it could be used directly by citizens. Funding to next stage implementation was granted to "Conflict Resolution with Equitative Algorithms 2" (CREA2), Grant Agreement 101046629,[310] in early December 2021 under the Justice Programme 2021-2027[311] with an official start in 2022.

- "Artificial intelligence for lawyers: Guide on the use of AI and other novel IT technologies by European lawyers and law firms" (AI4Lawyers), Grant Agreement 881527,[312] implemented by the European Lawyers Foundation together with the Council of Bars and Law Societies of Europe (CCBE).
- "Analytics for DEcision of LEgal cases" (ADELE), Grant Agreement 101007420,[313] implemented by Italian-Bulgarian Consortium. While the latter could be of particular interest as it applies legal analytics to judicial decisions to build a pilot tool to support legal research and decision-making processes in the judiciary, its activities are still in early stages and no prominent results can be discussed to date.
- "E-Justice ODR Scheme" (ODR e-Justice), Grant Agreement 101046468,[314] run by a European consortium, addresses the introduction of AI-related modules in ODR by preparing an open specification of standard civil judicial procedures and additional online dispute resolution procedures (e.g., mediation or arbitration). The project is aimed to start in 2022.

New e-justice calls shall continue to support AI projects in judiciary. The Justice Programme 2021-2027 first call's results are not yet fully published, but it is recommended to consider them for future developments.[315]

Reviewing projects exploring the impact of AI when used by judiciary, a project of particular interest is HUMAINT (Human Behaviour and Machine Intelligence),[316] run by JRC"s Centre for Advanced Studies in 2017-2020. To have a comprehensive understanding of the impact of AI on human behaviour, the research touches upon different sectors of society where AI may have a particularly large social impact, such as machine learning algorithms in decision making in the criminal justice system. The main case study on the latter was assessing the recidivism risk of defendants in Catalonia (Spain). Taking into account judges must consider the risk of the defendants fleeing or the likelihood to re-offend when

[310] Summary is available here. Project is running 2022-2024.

[311] Regulation (EU) 2021/693 of the European Parliament and of the Council of 28 April 2021 establishing the Justice Programme and repealing Regulation (EU) No 1382/2013, OJ L 156, 5.5.2021, p 21–38.

[312] Summary is available here. See also dedicated project website, where first project results are already published. Project is running 2020-2022.

[313] Summary is available here. See also dedicated project website, where first project results are already published. Project is running 2021-2023.

[314] Summary is available here. Project is running 2022-2024.

[315] Full list of funded projects shall be published here upon contract signing.

[316] https://ec.europa.eu/jrc/communities/community/humaint

they decide whether to detain or release defendants awaiting trial, the project compares the risk assessment tool Structured Assessment of Violence Risk in Youth (SAVRY) several machine learning models to assess how effective AI is at predicting the risk of recidivism, and whether it is fair.[317]

3.6.3 Specific Uses of AI in Criminal Law

While some of the ways in which AI-related practices have entered the courts relate to the calculation of the risks of misconduct (e.g., algorithmic probation, the use of predictive tools in criminal trials by judiciary), in general EU States refrain from exploring AI tools in criminal law. However, using such tools is heavily explored by law enforcement.[318] For example, the Dutch law enforcement authority has developed a machine learning AI-based system to identify old, unsolved, serious cases ("cold cases") that may now have good prospects of being solved.[319] Once the "cold case" files are digitised, they are fed into the AI system, which identifies those containing promising evidence that could be re-examined using new forensic techniques. Similar work conducted manually by police officers could take weeks of work per case, despite the likelihood of success being remote. The officers responsible for the project hope that it may be extended to identify "cold cases" that could be solved using non-forensic data, such as social science, social networks and witness statements. It might even prove capable of improving the police's ability to solve ongoing investigations into offences.[320]

At the same time, the use of AI in the judicial field appears to be quite popular in the United States, which has invested in such tools both in civil and criminal matters.[321] Controversies over AI tools used in criminal law in US further support the slow progress of such systems on EU ground. For example, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is a privately-owned system used in several US state jurisdictions to assess an individual's risk of reoffending. Being a web-based tool designed to assess offenders' criminogenic needs and risk of recidivism, it uses three "scales": "pretrial release risk" (i.e., risk of failure to appear and new felony arrest); "general recidivism" (commission of new misdemeanour or felony offences within two years); and "violent recidivism" (commission of violent offences).[322] The system raised a variety of concerns over the use of algorithms for criminal justice purposes refer to indirect racial bias in models that predict offending and re-offending, for instance by the use of proxy variables that are not neutral.[323] Another example can be given with the privately-owned PredPol system that was criticised for perpetuating historical bias in

[317] Gomez Gutierrez, E., Charisi, V., Tolan, S., Miron, M., Martinez Plumed, F. and Escobar Planas, M., Centre for Advanced Studies, Amran, G. editor(s), Publications Office of the European Union, Luxembourg, ISBN 978-92-76-28212-9, doi:10.2760/23970, JRC122667.

[318] See also European Parliament, 2020. "Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights" Study, PE 656.295, July 2020. Further analysis is provided in United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020, "Special Collection on Artificial Intelligence".

[319] Op. cit., RES 2342, pp. 13-14.

[320] "How the Dutch police are using AI to unravel cold cases", *The Next Web*, 23 May 2018.

[321] See also RES 2342, pp. 14-15.

[322] "Practitioners Guide to COMPAS", Northpointe, 17 August 2012.

[323] For example, see "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks", ProPublica, 23 May 2016.

policing practice, whilst at the same time concealing that bias behind a veneer or presumption of mechanical neutrality known as "tech-washing".[324]

UK has also fallen short on using the PredPol system,[325] yet the government is still experimenting with other forms of predictive policing. For example, nine forces led by West Midlands Police and including London's Metropolitan Police and Greater Manchester Police are developing the National Data Analytics Solution. The tool is being developed with technical support from a private company and use a combination of machine learning AI and statistics to assess, for example, the risk of someone committing or becoming a victim of gun or knife crime, as well as the likelihood of someone falling victim to modern slavery. The system is based on data relating to around five million individuals, from which it identified almost 1,400 indicators that could predict crime, of which 30 are particularly significant. [326]

Another UK example is the HART system developed by Durham Police with the support of Cambridge University. The system is aimed at supporting the prediction of reoffending and preventing recidivism. "Whilst Durham Police has stressed that HART is used only for advisory purposes and that individual decisions are the responsibility of trained police officers, some have been sceptical about how things will work in practice. As with Kent Police's use of PredPol, Durham chief constable Barton has revealed that repeated cuts to his force's budget have motivated increasing recourse to new technologies. These same cuts may have consequences for the availability of officers' time and attention, which is a significant factor in ensuring effective human responsibility for decisions made using HART." [327]

Progress has been made also in Russia,[328] Mexico,[329] and China[330] in exploring AI tools providing simple legal advice, such as how to bring a lawsuit or retrieve case histories, verdicts, and laws, or advising judges and clerks on plaintiffs' certain eligibilities. However, considering the lack of full alignment in terms of both ethical concerns and fundamental rights approach, the non-EU examples are not considered relevant for the Spanish reform's purposes; yet they could exemplify on a number of concerns and potential problems to be considered in delivering a solution compliant with EU legislation.

3.7 Recommendations

The draft law on digital efficiency under evaluation allows for the use of automated judicial actions (Articles 31-34 and following) in line with the requirements of the data protection regulation, mainly in the context of process and notification mechanisms automation. Furthermore, Articles 35-36 prescribe

[324] Op. cit., RES 2342, pp. 10-11.

[325] "Kent Police stop using crime predicting software", The Telegraph, 27 November 2018.

[326] "Exclusive: UK police wants AI to stop violent crime before it happens", New Scientist, 26 November 2018

[327] Op. cit., RES 2342, pp. 11-12.

[328] Zavyalova V, 2018. Save money on legal advice: AI is replacing lawyers in Russia. Russia Beyond.

[329] In Mexico, the Expertius system is advising judges and clerks regarding the determination of whether the plaintiff is or is not eligible for pension. See Carneiro D et al., 2015, Online Dispute Resolution: An Artificial Intelligence Perspective. Artificial Intelligence Review 41:227–228.

[330] World Government Summit, 2018. "Could an AI ever replace a judge in court?".

all systems used by judiciary to ensure proper structured data and metadata usage, in accordance with officially approved schemes and models to enable, simplify and favour – among others – the possibility for automated, assisted, and proactive judicial and procedural actions.[331] Application of AI techniques for the above purposes or others shall support the jurisdictional function, the processing and conclusion, where appropriate, of judicial procedures, and the definition and execution of public policies related to the judiciary. Following the overall context of the law,[332] it could be assumed that the use of AI tools shall be intended for purely ancillary administrative activities (such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, or administrative tasks) that do not affect the actual administration of justice in individual cases.

Nevertheless, considering the still ongoing debates on the AI Act and the introduction of AI tools in judiciary, we recommend the Spanish Ministry of Justice to reconsider the text in Article 35(k). Based on what is prescribed in the law, actions refer to automatization that does not necessarily imply use of AI techniques or tools. Thus, we believe that the AI reference should either be removed, or it should be made explicitly clear that such techniques should be restricted to purely ancillary administrative activities and low-risk activities in line with the risk-based approach undertaken by the AI Act.

In any case, a proper definition of what the Spanish legislator sees as AI should be provided if the term is used. Taking into account the controversies with regards to the AI Act's definition, we believe this will be a rather difficult exercise.

With regards to the above, we believe any national **legal framework** acknowledging or regulating the use of AI in judiciary shall be adopted, reflecting the overall framework of the AI Act; thus, it is recommended to consider specific legislative measures in the field of justice only after the adoption of the regulation. Taking into consideration the ongoing legislative reform in the Spanish justice domain, further enhancement of the law towards AI-related measures should be addressed only when proper evaluation of clauses dedicated to semi-automated and automated actions are evaluated within a year after the entering into force of the respective legal texts.

A review of the strategic and policy approach shows that high-risk activities are considered better addressed by legislation and self-regulation ex ante than by post facto judicial intervention. At the other end, low-risk activities are seen as not necessarily requiring dedicated legislation, and can be addressed through existing legislation, standards, and self-regulation. In any case, regulation of AI, whether voluntary self-regulation or mandatory legislation, should be based on universally accepted and applicable core **ethical principles**: transparency, including accessibility and explicability; justice and

[331] Based on Explanatory document of the draft law on digital efficiency of the public service of the Administration of Justice, provided by the Spanish Ministry of Justice, "assisted, proactive and automated actions are also regulated. Automated actions, already defined in Law 18/2011, are favoured, and regulated, making specific provisions for their uses for repetitive and automatable tasks (pagination of files, declaration of firmness, for example), but also establishing limits. It will also regulate assisted and proactive actions. The former generates a total or partial draft of the text, which can support the task of the Judge, Prosecutor or LAJ, always maintaining full control over it. The latter takes advantage of the information incorporated for a specific purpose, to generate effects or notices for other purposes. For example, notifications or automatic reminders."

[332] Since the text has been translated into English, its interpretations shall be reviewed under scrutiny.

fairness, including non-discrimination; human responsibility for decisions, including liability and the availability of remedies; safety and security; and privacy and data protection.

Furthermore, when introducing any AI-related measures and/or AI tools, the newly adopted CEPEJ's "Guidelines on electronic court filing (e-filing) and digitalisation of courts"[333] should be considered and the implementation of such solutions in judiciary should be understood as a systemic and comprehensive reform – that goes well beyond the technological and part of **a complete ecosystem of services**, rather than one or more separate projects with a firm timing of implementation. In this regard, drafting a clear roadmap (stand-alone or embedded document) indicating details on the necessary changes and expected impacts is recommended.

An effective and efficient AI-based transformation programme requires strong political will, all-embracing management approach, and **broad stakeholder involvement** (including civil society organisations and community representatives). All measures should be continuously adjusted to reflect the needs of various stakeholders of the justice system, be they internal or external users. Complementing change management measures to promote a mindset for continuous improvement could be introduced.

The design of an AI-dedicated roadmap should engage users and allow every stakeholder to submit feedback from the very beginning of the process. Such co-optation guarantees the involvement of internal and external users along the way and provides an opportunity for more **collaborative, participatory, and transparent AI implementation**. When confronted with juridical processes, citizens often have difficulties navigating the legal system.[334] In this context, AI measures can be dedicated to making juridical processes more **explainable and accessible to citizens**.

Before introducing AI solution, the Spanish Ministry of Justice shall guarantee that **internal expertise** able to evaluate and advise on the introduction, operation and impact of such systems is available long-term, to ensure that every new application of AI is justified, its purpose specified and its effectiveness confirmed before being brought into operation, considering the operational context. Hence:

- **Clear requirements** for algorithmic impact assessment, transparency, quality assurance, recourse, and reporting shall be set depending on the specifics of the technology used and the context of its application.
    - Regulatory sandboxes or other testing initiatives could successfully support all development stages.

[333] European Commission for the Efficiency of Justice (CEPEJ), 2021. Guidelines on electronic court filing (e-filing) and digitalisation of courts, CEPEJ (2021) 15REV2. Adopted at the 37th plenary meeting of CEPEJ, 9 December 2021.

[334] Confirmed by a recent study in UK, finding that 70% of consumers would prefer using an automated online system to handle legal affairs instead of a human lawyer because of three important factors: speed, cost, and ease of use. Such online systems include solutions ranging from AI-powered chatbots to comprehensive AI guides that walk individuals through critical decisions that need to be made for their circumstances.

- Model rules on impact assessment could be adopted, in case decentralised management of AI projects across judicial authorities shall be allowed.

– **Independent oversight mechanisms** for the introduction and operations of all AI systems shall be established.

– Introduction, operation and use of AI applications shall be always subject to **effective judicial review**.

Final decision-making must remain a **human-driven activity and decision**. Considering the current stage of technology development, only a judge can guarantee genuine respect for fundamental rights, balance conflicting interests and reflect the constant changes in society in the analysis of a case. It is also important that judgments are delivered by judges who fully **understand the AI applications** (where any decision-making support is provided by such) and all information considered therein that they might use in their work, thus, they can explain their decisions. In this regard, the use of AI applications must not prevent any public body and/or official from giving explanations for their decisions. Importance should be placed on the **training** of judges and prosecutors on the use of AI applications.[335]

[335] European Commission, Communication, Ensuring justice in the EU — a European judicial training strategy for 2021-2024, COM (2020) 713.

4 Online Alternative Dispute Resolution

Alternative dispute resolution (ADR) refers to an out-of-court dispute resolution mechanism with the assistance of an impartial dispute resolution body, without recourse to litigation. CEPEJ glossary refers to arbitration, conciliation, mediation, and court-annexed mediation.[336] The terms "online dispute resolution" (ODR) and "online alternative dispute resolution" (online ADR) refer to mechanism for resolving disputes through the use of electronic communications and other information and communication technology.

4.1 Status Quo on ADR

Research shows the Spanish Arbitration Law passed in 2003 establishes a favourable legal framework for arbitration providing for an efficient and flexible dispute resolution mechanism. Spanish awards[337] are immediately enforceable, even if a request to set aside the award has been filed. The Arbitration Law provides that Spanish awards may only be set aside on the following grounds: the arbitration agreement does not exist or is void; the party challenging the award has not been given proper notice or opportunity to present its case; the arbitrators have ruled on questions not submitted for their consideration; the composition of the arbitral tribunal or the arbitration proceedings has been irregular; the arbitrators have decided on questions that cannot be settled by arbitration; or the award is contrary to public policy. The action to set aside the award is not an appeal and therefore does not entail a review of the merits of the case. Spanish case law is consistent with this approach, making clear that the scope of review in proceedings to set aside an award is strictly limited to verifying that the essential principles of due process have been observed during the arbitration.

The Arbitration Law was amended in 2011 (ref. Law 11/2011). The amended Law retained the fundamental pillar of arbitration (namely, party autonomy), yet unifying case law and guaranteeing greater legal certainty. The (limited) competence for judicial control of arbitration was concentrated in the High Courts of Justice.[338] The role of supporting arbitration (except the judicial appointment of arbitrators) falls to first instance courts, as they continue to assist in the taking of evidence, the judicial granting of interim measures and the enforcement of awards.

With regards to mediation, it is regulated as an alternative to judicial proceedings and arbitration by Law 5/2012 on mediation in civil and commercial matters transposing Directive 2008/52/EC[339] into Spanish law. Criminal mediation, mediation with public authorities, labour mediation or mediation in consumer matters fall out of scope. The final agreement or settlement under Law 5/2012 is binding on the parties and can cover all or only part of the matters subject to mediation; if the parties wish it to be

[336] European Commission for the Efficiency of Justice (CEPEJ), CEPEJ Glossary, CEPEJ (2020) Rev1, p. 5.

[337] The enforcement of foreign awards in Spain is governed by the 1958 Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention"). Spanish courts favour simplicity and expeditiousness when enforcing foreign awards.

[338] It is within High Courts of Justice's authority to hear actions for annulment of arbitral awards rendered in arbitrations where Spain is the seat of arbitration and to hear requests for recognition of foreign awards.

[339] Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters, OJ L 136, 24.5.2008, p. 3-8.

enforceable, the agreement must be converted into a public deed. In December 2013, Royal Decree 980/2013 was approved, developing specific aspects of Law 5/2012.

Spanish legislation on consumer alternative dispute resolution systems for consumer disputes, transposing Directive 2013/11,[340] was adopted in 2017 (ref. Law 7/2017) to ensure access for both Spanish and European consumers to independent, impartial, transparent, and effective alternative dispute resolution mechanisms in Spain. Law 7/2017 sets out that traders must inform consumers of the existence of ADR entities. The information obligation should be fulfilled as follows: (a) traders adhering to an authorized ADR entity or those who are bound by a rule or code of conduct to accept the intervention of an ADR entity in case of consumer disputes must inform consumers about the possibility of submitting their dispute to that entity; the information shall include a full identification of the ADR entity and shall be provided in a clear and identifiable way and included in the general terms and conditions that govern the sale or service provided to consumers; and (b) traders that provide online sales or service, e-commerce platforms and online markets, must include in their website a link to the European online dispute resolution platform. Law 7/2017 also states that when a claim is submitted to any ADR entity, prescription and expiration periods shall be interrupted or suspended as established at the applicable regulation; and sets out that any dispute shall be solved within a maximum period of 90 days from the receipt of the consumer's complaint and that the final decision to an ADR mandatory procedure does not prevent the possibility of taking a common action in court. Further, the Law establishes the requirements that Spanish ADR entities shall meet to be recognized as authorized ADR entities, the authorization procedure and other aspects related to the ADR procedure such as costs (the procedure itself shall be free for consumers).

In addition to arbitration and mediation, another instrument considered as a valid alternative to litigation in Spain is the so-called expert determination. This is a flexible procedure for the resolution of disputes based on the decision of an independent third party and is regarded as especially suitable for factual disputes or disputes in which a high degree of technical knowledge is required.

With regards to the application of web-based technology to ADR, Article 24(2) of the Spanish Law 5/2012 already encourages such application ("Mediation as a matter of a claim not exceeding EUR 600 shall be carried out preferably by electronic means unless the use of such a complaint is not possible for any of the parties").

Considering ODR for consumer disputes, Spain applies Regulation (EU) No 524/2013[341] concerning out-of-court claims initiated by consumers resident in the EU against traders established in the EU which are covered by Directive 2013/11/EU. Obligations for online platforms to engage with certified out-of-court dispute settlement bodies to resolve any dispute with users of their services are to be regulated

[340] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), OJ L 165, 18.6.2013, p. 63-79.

[341] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), OJ L 165, 18.6.2013, p. 1-12.

by the future Digital Services Act.[342] Thus, the ODR for consumer disputes[343] and out-of-court dispute resolutions applicable to online platforms fall out of scope of the present analyses and will need to comply with the requirements of the EU legislation to be adopted. Given the EU legislative process on the Digital Services Act the authors cannot speculate on the outcome of the ongoing interinstitutional discussion.

4.2 Towards ODR

In 2016, United Nations Commission on International Trade Law (UNCITRAL) adopted the Technical Notes on Online Dispute Resolution[344] recommending that all States and other stakeholders use this document in designing and implementing ODR systems for cross-border commercial transactions. The Technical Notes are a non-binding, descriptive document, reflecting on elements of an online dispute resolution process in line with the principles of impartiality, independence, efficiency, effectiveness, due process, fairness, accountability, and transparency; describing the stages of an ODR proceeding (negotiation, facilitated settlement, and a third (final) stage) and how technology shall be used to enable a dispute resolution process at each of these stages; and recommending the development of guidelines (and/or minimum requirements) in relation to the conduct of ODR platforms and administrators to better facilitate the ODR governance processes.

The Working Group on Cyberjustice and Artificial Intelligence of the European Commission for the Efficiency of Justice (CEPEJ) to the Council of Europe (in short, CEPEJ-GT-CYBERJUST) is currently working on providing guidelines on online alternative dispute resolution for the Council of Europe member States. These guidelines are currently under revision;[345] thus, the present analysis only acknowledges the preparatory work done so far based on a review of 32 ODR providers worldwide. Most important conclusions refer to:

- Most countries do not have specific legislation or government regulation specifically applicable to ODR. Exceptions to be considered are, for example, Italy, where soft regulation on video conferencing in ADR is present, or France, where there is an ongoing process of reforming ODR at the moment.
- Different platforms and procedures on rendering ODR services apply, with most ODR providers utilizing popular market platforms for online communication.

[342] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM (2020) 825 final.

[343] Exemplary best practices towards potential improvement in this regards can be found in the Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes, COM/2019/425 final.

[344] UNCITRAL Technical Notes on Online Dispute Resolution, New York: United Nations, 2017.

[345] European Commission for the Efficiency of Justice (CEPEJ), Report from the 4th meeting of CEPEJ-GT-CYBERJUST, CEPEJ-GT-CYBERJUST (2021) 8.

- In most cases there is no mechanism for digital enforcement of the results reached in ODR proceedings.[346]
- There is no uniformity with regards to documentation maintained on the ODR cases.
- Only 40% of the researched ODR services envision the potential use of (some kind of) electronic signature.
- Around 30% of the surveyed ODR services declare using AI techniques in the core part of the process (i.e., in resolving the issue submitted to parties).
- There is no uniform practice or approach to ensure confidentiality in the digital environment, while a variety of measures is used to compensate to a certain extent.

The draft ODR guidelines are being developed reflecting on the need for a dedicated tool to support member States and ODR providers in the implementation of efficient systems respectful of human rights and in line with European standards. In its 4th plenary meeting, CEPEJ-GT-CYBERJUST has confirmed the focus of the guidelines should fall on particularities of online procedures in the alternative dispute resolution process, remaining horizontal, thus without going specifically into criminal procedure, restorative justice, or family matters, due to limits in its actual application. A stronger focus should be given to safeguards for vulnerable groups. Furthermore, the ODR guidelines under preparation are expected to complement the guidelines on online dispute resolution mechanisms in civil and administrative court proceedings,[347] already prepared by the European Committee on Legal Co-operation as regards the specific aspects of ODR in court proceedings, providing member States with guidance in relation to: fair procedure (access to justice, equality of arms, evidence, effective proceedings, delivery of the decision, right to a reasoned decision, enforcement of the decision, right to judicial review in cases involving purely automated decisions); transparency in the use of ODR and requirements for hearings; as well as special issues related to the ICT nature of ODR techniques (cybersecurity and human rights protection, including personal data protection).

The CEPEJ Mediation Working Group (CEPEJ-GT-MED) has also offered its thoughts on the contribution of information technology towards alternative dispute resolution methods. In their 2019 handbook for mediation law-making,[348] the inclusion of electronic means to the process is encouraged. It is considered that the use of electronic means can increase the accessibility of the process by using various types of video and teleconferencing solutions in order to reduce the need to travel and, subsequently, the costs of mediation, and with regards to the fact that negotiation tools may help the mediator and the parties to prioritise and find better-adjusted solutions in a shorter period.[349] The handbook mentions several national laws already referring to the possibility of using electronic means

[346] Authors of the study mentioned only one example for a potential online enforcement mechanism using an escrow account.

[347] Council of Europe, 2021. Guidelines on online dispute resolution mechanisms in civil and administrative court proceedings. See also the Explanatory Memorandum to the Guidelines.

[348] European Commission for the Efficiency of Justice (CEPEJ), European Handbook for Mediation Lawmaking, CEPEJ (2019) 9.

[349] Ibid, p. 62.

in mediation (e.g., Cyprus,[350] Italy,[351] Lithuania[352]). Further, it advises mediation providers using electronic means to ensure that procedural requirements for mediation and the conduct of mediator are met regardless of the form of mediation chosen. Such approach can either be ensured by placing a reference in the respective rules of the mediation provider (e.g., in Italy) or in the respective legal act (e.g., in Spain, where mediation can only be carried out provided that the identity of the parties concerned is ensured and compliance with the principles of mediation laid down in the law[353]. Nevertheless, online mediation shall not remain the sole way of settling disputes and parties shall remain free to choose which method (electronic or traditional in presence) to apply during mediation.

With regards to ICT tools used in practice, ODR can vary greatly in terms of both techniques and technology, be they used separately or in combination, such as online platforms directly accessed and used by the parties and/or their representatives for the filing of statements and procedural documents; online platforms for storing, processing, assessing and presenting documents and evidence in electronic format; or online communication platforms allowing for the giving of oral testimony of witnesses and experts. With regards to communication, both remote asynchronous[354] and synchronous[355] methods can be used to optimize the flexibility and convenience of communication and/or with regards to holding online hearings.

Use of artificial intelligence in recent days is common, yet contradictory. More on the use of AI in automation of proceedings and applicable safeguards is available in Section 3 on automatization of decisions using AI, part of the present report. Two projects mentioned, namely CREA2 and ODR e-Justice, may present a particular interest in future considering the potential of their outcomes.

Another emerging application of technology refers to the use of smart contracts and blockchain in arbitration, for automating or designing the resolution processes. Unlike regular contracts, smart contracts are written entirely in code and allow for the automatic execution or enforcement of obligations. However, further regulation of smart contracts is needed to provide for undisputed ODR solutions, especially in cases where national legislations do not recognise smart contracts as valid contracts. Further discrepancies may appear when translating complex contracts into smart contract codes.

Although the use of technology could successfully support the provision of ADR online, aspects such as trust, authentication (validating the identity of the party and the legal validity of their digital signatory), data security and confidentiality, privacy, and post-resolution compliance, remain problematic. These issues should be addressed when an ODR framework of requirements is drafted with appropriate

[350] The Republic of Cyprus, The Certain Aspects of Mediation in Civil Matters Law. Official Gazette, Supplement 1(I): 16.11.2012, No. 4365, 2012 No. L.159 (I)/2012.

[351] The Republic of Italy, Legislative Decree of March 4, 2010, n. 28, Art. 3 (4).

[352] The Republic of Lithuania, Law on Mediation. Valstybės žinios, 2008, No. 87-3462; Teisės aktų registras, No. 2017-12053.

[353] The Kingdom of Spain, Law on Mediation in Civil and Commercial Matters. Boletín Oficial del Estado, No. 5/2012, Art. 24(1).

[354] E.g., discussion boards, blogs, email, various forms of secure and authenticated databoxes guaranteeing the authenticity and integrity of a communication, etc.

[355] E.g., chat, instant messaging, audio- and video-conferencing tools, etc.

legislative, organizational and technical measures. Yet, since ODR providers might be both private and public bodies, such a framework shall acknowledge the jurisdictional specificities of the respective scheme.

4.3 Recommendations

With regards to the draft law on digital efficiency under evaluation,[356] the legislator has not yet included any specific provision in the text regarding ODR. However, considering the reform undertaken by the Spanish Ministry of Justice, it could be assumed that similar measures on digital efficiency shall be established to support public or state-funded ADR entities in effectively providing ODR services in relation to fair procedure, transparency in the use of ODR, as well as special issues related to the digital nature of ODR.

To increase legal certainty and reinforce certain values, a framework secondary legislation on online ADR proceedings could be introduced, with the aim to:

- reflect on the key principles to be followed with regards to impartiality, independence, efficiency, effectiveness, due process, fairness, accountability, and transparency, and how they shall be followed in an online environment;
- propose organizational and technical aspects to ensure fair procedure, thus avoiding potential violations of the European Convention on Human Rights;
- advising on proper allocation of funding and efforts ensuring all-inclusive compliance throughout testing, development, deployment,[357] monitoring and upgrading ODR tools;
- mitigate risks of erroneous or unjustified blocking speech, stimulate the freedom to receive information and hold opinions, as well as reinforce parties' redress possibilities;
- mitigate discriminatory risks considering the needs of specific groups or persons that may be vulnerable or disadvantaged in their use of online services because of their gender, race or ethnic origin, religion or belief, disability, age, or sexual orientation, and contribute to the protection of the rights of the child and the right to human dignity online;
- impose mandatory safeguards related to cybersecurity,[358] protection of personal data,[359] and protection of parties' information, including the provision of explanatory information to the user, complaint mechanisms supported by the service providers as well as external out-of-court dispute

[356] Since the text has been translated into English, its interpretations shall be reviewed under scrutiny.

[357] Especially in the context of deployment commercial off-the-shelf products.

[358] E.g., safeguards against unauthorized access to confidential information, unwanted alteration or deletion of data, technical impossibility to access systems or data by those should have such access, uncertainty against the identity of the ones involved in the dispute resolution process, identity fraud, etc.

[359] In compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.

resolution mechanism; parties shall be informed in a clear and comprehensible manner whether the processing of their dispute is done in an entirely automated way or with the involvement of a mediator or arbitrator;

- considering the enforceable nature of the award, impose certain technical requirements to the various stages of the ODR proceedings to ensure the validity of the procedure and the award itself;
- prescribe the introduction of an enforcement mechanism;
- encourage awareness raising and/or training on using ODR mechanisms and tools.

Yet, such legislation can only provide framework clauses. Self-regulation in the form of detailed ODR rules and/or voluntary sectoral codes of conduct shall be encouraged within the context of a common legal frame.

In any case, ODR services need to comply with existing Spanish legislation on ADR.

With regards to cybersecurity, the EU Cybersecurity Act[360] introduces an EU-wide cybersecurity certification framework for ICT products, services, and processes. Entities doing business in the EU will benefit from having to certify their ICT products, processes, and services only once and see their certificates recognised across the European Union; thus, such voluntary certification could also be encouraged for public or state-funded ODR services.

[360] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15-69.

5 Remote Hearings (Telematic Trials)

This topic is related to hearings that take place via videoconference.

This chapter reports the result of the analysis of existing national regulations and best practices in some countries, focusing on the following sub-topics:

- Broadcasting a trial via internet (to general public), accessible after user authentication and authorization
- Security of remote witnesses, eventually placed in secure spaces
- Legal validity in case of exception or appeal (procedures/practises to provide technical info).

For each sub-topic, the answers provided to the survey by some Member States of the Council of Europe (in the section "Remote court hearings") are considered; desk research has been performed on other European and non-European countries providing interesting situations or experiences.

Furthermore, a focus on CEPEJ "Guidelines on videoconferencing in judicial proceedings"[361] (VC Guidelines) and on the provisions of the current draft of the Law on Digital Efficiency is made. Comments and recommendations, that might be considered in the Law or in other secondary legislation, are finally provided.

5.1 Broadcasting a Trial via Internet

This sub-topic is related to the possibility for the public to participate in remote hearings, thus ensuring the principle of "open justice" and accomplishing the right for the citizens to effectively participate to trials.

The research is also focused on how the access is granted to the public, i.e., if there's the need for identification (authentication) and authorization mechanisms.

5.1.1 Information from Other Countries

On this topic, the Survey among some member States of the Council of Europe explored on the issues of national legislation (be it in force or under preparation) or established best practices that cover the following aspects related to remote court hearings:

- Participation of the general public to remote hearings in real time? (ref. Item 2.4 of the Survey)
- Access of the general public to the recordings of remote hearings? (ref. Item 2.5 of the Survey)
- If the reply to any of the above questions is "Yes", are there authentication or authorisation mechanisms in place? (ref. Item 2.6 of the Survey)

The following tables summarizes the answers provided:

[361] Adopted by the CEPEJ at its 36th plenary meeting (16 and 17 June 2021): https://rm.coe.int/cepej-2021-4-guidelines-videoconference-en/1680a2c2f4

Country	2.4	2.5	2.6	Comment (to specific topic)
Cyprus	No	No	No	-
Austria	**Yes**	No	No	Participation of the general public to remote hearings is just possible in the court which handles the case
Ireland	No	No	No	-
Switzerland	**Yes**	No	**Yes**	[translated from French] Current legislation only authorizes the use of videoconferencing in criminal proceedings. Little use is made of this possibility. The answers given reflect the most common practices.
North Macedonia	**Yes**	**Yes**	**Yes**	All issues to be included in the Law on criminal procedure and in the Judicial rules of procedure.
Slovakia (Ministry of Justice)	No	No	No	-
Luxembourg	No	No	No	-
Germany	No	No	No	(2.4, 2.5) The participation of the general public always requires physical presence in the court. There is no streaming of court hearings to a remote public, neither live nor recorded
Monaco	No	No	No	-
Bosnia and Herzegovina	No	No	No	-
Sweden	No	No	No	All statements given in criminal and civil cases are recorded on video, there is no difference if the person heard is present in the court room or attending via video. The general public has access to the courtroom where the cases is tried, and where the person heard via video appears on screens. There are no hearings in Sweden that are completely remote, there is always a physical place where the hearing takes place and that the general public has access to. No video recordings from court hearings are accessible to the general public - but the audio recordings are public documents that everyone has access to.
Norway	**Yes**	**Yes**	No	when it comes to the publics access to recordings we have a pilot which record parts of the hearing and the legislation will regulate the publics access
Latvia	**Yes**	**Yes**	**Yes**	-
Lithuania	**Yes**	No	**Yes**	-
Slovakia (IT project manager)	No	No	No	-

The Netherlands	**Yes**	**Yes**	**Yes**	Online court proceedings in the Netherlands take place in all areas of law, but particularly in administrative and civil law cases. Participation in such hearings by request. In criminal law cases court hearings ('telehoren') can be arranged in some cases, with no option to remotely access the hearings
Ukraine	No	**Yes**	No	-
Slovenia	No	No	No	-
France	No	No	No	-

Upon direct request to the contact points that provided the answers, some clarifications follow:

- Austria: The current approach is largely ensured by an organizational framework. Planned remote court hearings are always carried out with a participant in an on-site courtroom (even if only in the form of a passive transmission that is set up by court staff). In this regard, there is no specific legislation for public access to remote court hearings in place.
- Switzerland: When there are court hearings with a lot of people and there is not enough place in the court room, some courts have in a recent past transmitted via a videoconferencing system the hearing in a bigger room close to the court room, so that the public can follow the hearing live. The identification is physical, like the one needed to access the court room, made by the court's staff. There is no specific legislation to allow transmission of hearings from the court room to other rooms.
- Latvia clarified that persons wishing to participate in the hearing as listeners (media included) shall apply to the court that they wish to participate in the public hearing: the court shall send the same link with the ID and password to the hearing as transmitted to the party.[362]
- Lithuania clarified that the public may participate connecting to Zoom or MS Teams platforms. In such case, the person willing to participate should inform the court in advance (no later than three working days before the date of the hearing) and ask for the link to participate. There's no specific legislation, but provisions are contained in the "Recommendations on Remote Court Hearings" adopted by the Council of Judges on 27 August 2021, which also gives the possibility to retransmit the sound of the hearing and (if possible) the image to a separate court open to the public or to another room in the same court building.

At the European Court of Human Rights (ECHR), to preserve the public character of hearings by videoconference,[363] all public hearings are filmed and broadcast on the Court's website. Hearings held in the morning can normally be viewed as of 2.30 p.m., while afternoon hearings are available at the end of the day, barring technical difficulties, usually with interpretation in French and English.[364] The

[362] Criminal Procedure Law, Section 140. and further sections. Civil procedure law Section 155.

[363] Article 40 of the Convention, Rule 63 of the Rules of Court

[364] https://www.echr.coe.int/Pages/home.aspx?p=hearings&c=

first remote Grand Chamber hearing took place on 10 June 2020: there were four remote locations connected to the courtroom.[365]

As per direct knowledge of one of the experts, in Italy for criminal trials that take place in videoconference it is necessary that judges, prosecutors, and lawyers are physically present in the courtroom, while the defendants that are in prisons are connected from equipped rooms in the prisons. The system is highly secured and not connected to the internet, so the public can only be physically present in the courtroom. For trials of mediatic importance, where a massive participation of public and media is expected, other courtrooms (connected to the same system) can be used to host people.[366]

In Poland, court in Łodź issued ordinance allowing for public participation in remote hearings via the Internet. An electronic admission card, issued by the court upon request, is needed. The link to connect to the hearing (via Microsoft Teams) is sent via mail and is encrypted, so that only the recipient can use it. Along with the electronic admission card, a brief information is sent on the prohibition of image and sound recording and the obligation of the public to maintain solemnity, peace, or order of court activities.[367]

Restrictions imposed during the COVID-19 pandemic in England and Wales accelerated the use of digital technology for remote hearings.[368] The relevant provisions of the Coronavirus Act have been carried over into the Police, Crime, Sentencing and Courts Bill 2021, with a view to making the changes permanent. According to the explanatory notes, the intention is for the detailed working of the provisions to be managed, and updated, under secondary legislation. The bill also provides for jury trials[369] to be held remotely (but only by live video link) and for further use of live video links generally.[370]

In early April 2020, two experimental virtual jury trials took place in England.[371] To recreate the public gallery, the virtual court hearing was streamed on YouTube and a link was provided to allow invited observers to view it live. Observers were invited from HMCTS, the Bar Council, Criminal Bar Association, and the media to view the experiment; the virtual courthouse created mirrored courthouses in HMCTS estate by having a public frontstage and a backstage with private facilities to which the public had no

[365] https://www.echr.coe.int/Pages/home.aspx?p=hearings&w=669718_10062020&language=lang&c=&py=2020

[366] For earlier experiences with video technology in courtrooms in Italy, see Chapter 5 – "Experimenting with Video Technology in the courtroom", in Giovan Francesco Lanzara, *Shifting Practices. Reflections on Technology, Practices, and Innovation*, The MIT Press, 2016, p. 151-174.

[367] https://lodz.sr.gov.pl/posiedzenia-online,m,mg,346

[368] https://www.tandfonline.com/doi/full/10.1080/17577632.2021.1979844

[369] Jury trials are held in criminal cases in crown courts.

[370] See proposal for to amend Section 51 Criminal Justice Act 2003 (available at https://bills.parliament.uk/publications/43970/documents/1042). For a broader view of the legislative process see https://bills.parliament.uk/bills/2839/publications

[371] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876199.

access (i.e., jury room, virtual private space where the defendant could consult with their counsel,[372] virtual room in which the prosecutor was able to introduce themselves to the witnesses, a fourth space was created for Jurors, the clerk and Judge in the form of a private chat function). While the trial was taking place all the parties had exactly the same "shared" screen view.

Interesting lessons learned were:

- microphones could also be controlled by an operator which reduced the likelihood of jurors speaking over anyone else;
- a new screen indicating when the court was not in session was added to limit what the public were able to see in the courtroom during times when technicians were "bringing" people in and out of the virtual court. The screen also provided some reassurance about what was happening for participants trying to re-enter the trial after a break or jury deliberations.

This experiment was also the chance to raise the concern about what would happen if members of the public are allowed open access to live streamed proceedings because of their ability to record proceedings or take photographs of those involved (in England, photography in court is banned under the Criminal Justice Act 1925).

Furthermore, selected cases from the Court of Appeal (Civil Division) are now being live-streamed on the judiciary's YouTube channel. Watching some of the videos in their archive, it can be noted that some of the hearings during the pandemic were taken via Microsoft Teams, basically sharing the virtual room; the audio of some of those is low or bad and not always synchronized with video.[373]

The Coronavirus Act 2020 expanded the availability of video and audio link in court proceedings.[374] It allows certain civil applications in the magistrates' court to take place by phone or by video, expands the availability of video and audio link in some criminal proceedings, and permits the public to participate in court and tribunal proceedings through audio and video links.

With regard to civil proceedings, a pilot was established to run between 2 March 2020 and 31 March 2021 at Birmingham and Manchester Civil Justice Centres for proceedings default judgments and proceedings seeking to set aside default judgments and where the email address of the parties or of their representatives are known to the court.[375] In these situations the court could require the parties to attend the hearing online. In preparation for this a procedure would need to be followed (Para 2(2) Practice Direction 51V):

- at least 14 days before the hearing date, each party or legal representative has to complete, online, a pre-video hearing suitability questionnaire, the link to which will be provided by the

[372] Ensuring the link is secure, integrated in the same platform and that technicians cannot hear what is being said is clearly an imperative for any designers.

[373] https://www.youtube.com/watch?v=xM77u7Tu1MA

[374] https://www.gov.uk/government/publications/coronavirus-bill-what-it-will-do/what-the-coronavirus-bill-will-do#contents-of-the-bill

[375] Para 1 Practice Direction 51V – Video Hearings Pilot Scheme (available at https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part51/practice-direction-51v-the-video-hearings-pilot-scheme).

court, which provides for unrepresented parties to consent to the application proceeding by way of video hearing, and for represented parties to let the court know anything that could affect this hearing taking place by video (including whether the party objects to or wishes to opt out of a video hearing);

- a court officer has to consider the completed pre-video hearing suitability questionnaires and to be satisfied that each party or legal representative is able, and has access to the IT equipment required, to participate in a video hearing;
- a judge has to consider both the application and the completed pre-video hearing suitability questionnaires and has to determine that the application may proceed by way of a video hearing;
- at least 7 days before the hearing date the court has to set-up the video hearing user account for each party or legal representative and test the IT equipment used for each party or representative and confirm that it will enable them to access the court hearing.

If following testing the conditions for an appropriate video hearing are not met the rules establish that the hearing will have to take place in person. This is to guarantee the appropriate handling of the proceedings.

Specific transitory arrangements regarding video or audio hearings have been adopted for the period of COVID-19 pandemic (Practice Direction 51Y).[376] According to these rules the courts are to carry out proceedings wholly as a video or audio proceedings. As a result, the hearings are set to be private unless it is possible to have hearings broadcasted in accordance with Section 85A Courts Act 2003[377] in court buildings or a media representative is able to access the proceedings remotely. The hearing held in private is to be recorded to enable the court to keep the audio-video record of the proceedings based on Sections 85A of the Courts Act 2003.[378] Since the start of the COVID pandemic more court rooms were equipped with video hardware – Cloud Video Platform (CVP) to ensure courts could still hold hearings. Her Majesty Courts and Tribunals Services (HMCTS) developed a Video Hearing service specifically designed to meet the needs of the judiciary and of court and tribunal users. The Video Hearings Service is set to support the users in advance of their hearing, informing them on what to expect on the day. The interface for the hearing has been developed and designed to replicate the formality of the court proceedings.[379] The Video Hearings Service is being used in tax, property and employment tribunals and is being tested in civil and family hearings. The service is expected to continue to run also after the COVID emergency with the judge considering whether in specific cases and given their complexity it is appropriate to continue via a remote hearing or parties should be

[376] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part51/practice-direction-51y-video-or-audio-hearings-during-coronavirus-pandemic.

[377] https://www.legislation.gov.uk/ukpga/2003/39/section/85A.

[378] https://www.legislation.gov.uk/ukpga/2003/39/contents.

[379] https://insidehmcts.blog.gov.uk/2021/06/09/remote-hearings-their-role-in-extending-access-to-justice/.

present in court or in a hybrid form (some parties being present in court and others accessing from a remote location).[380]

In the Netherlands, there is a difference between the usual court proceedings and the special procedure established for the International Commercial Court (special chamber of the Amsterdam District Court) that is accessible in commercial claims based on a specific choice of court agreement by legal parties. Following the COVID-19 health emergency special rules were established in order to allow courts to continue holding hearings.[381] If a remote hearing is decided to take place, the court via its Judiciary Service Centre (*Het Rechtspraak Servicecentrum*, RSC) will contact the parties that should attend by email to arrange and test the technical details. Such hearings can take place via various applications such as Teams, Skype (via pc, tablet, app or telephone), CMS or via telephone.[382] If the party to be heard does not have access to internet, the party is allowed to connect to the video hearing together with her lawyer or the court will seek to make other arrangements such as securing the participation of the party by telephone. If documents are to be shown during the online hearing the judge has to give permission in this regard if Teams or Skype are used.[383]

In the special proceedings before the International Commercial Court the judges were faced with one issue: "some members of the public wanted to remain anonymous. We decided to apply the ordinary courtroom hearing rules: accordingly, members of the public must be on screen and viewable by the parties. Therefore, we require that anyone from the public wishing to attend must switch on their camera. We are contemplating options for live feeds from hearings. A review of relevant data protection and other rules is in progress."[384]

In some European countries, especially those where filming hearings is forbidden, there are reservations about streaming hearings.[385] As reported in the article entitled "Video-Hearings in Europe Before, During and After the COVID-19 Pandemic" by Anne Sanders,[386] "in personal conversations, German judges expressed their fear that streaming hearings would lead to attacks on judges via social media. If streaming hearings, or at least all hearings, is not an option, public access must be secured in other ways. […] In respect of access of the public and the media to remote hearings, there is still a need

[380] https://insidehmcts.blog.gov.uk/2021/06/09/remote-hearings-their-role-in-extending-access-to-justice/.

[381] The latest temporary rules related to physical or online hearings are available at https://www.rechtspraak.nl/coronavirus-(COVID-19)/Paginas/COVID-19-tijdelijke-algemene-regeling-zaaksbehandeling-Rechtspraak.aspx#b032923c-801f-4698-a478-1c52448fd251a32b6908-c069-45db-a355-94c5665ca9a960. See also https://www.rechtspraak.nl/coronavirus-(COVID-19)/Paginas/tijdelijke-regelingen.aspx .

[382] Information and explanations on online hearings are available at https://www.rechtspraak.nl/online-zittingen-en-overleggen#fa8e8bd2-c7b7-418c-ac27-bc672c2a18cad4c1ac22-f39f-4267-9096-58686564f69383.

[383] This is not the case if the CMS application is used for the hearing. See https://www.rechtspraak.nl/online-zittingen-en-overleggen/Paginas/Veelgestelde-vragen-online-zittingen-en-overleggen.aspx#4bf90a53-8a61-4492-9300-cd2e2cd023c1d4c1ac22-f39f-4267-9096-58686564f69372.

[384] https://www.rechtspraak.nl/English/NCC/news/Pages/The-Netherlands-Commercial-Court-and-COVID19-case-management-videoconference-hearings-and-eNCC.aspx

[385] D. Kettiger, Gerichtsverhandlungen, Anhörungen und Einvernahmen mittels Videokonferenz, Jusletter 4. Mai 2020

[386] https://www.iacajournal.org/articles/10.36745/ijca.379/

for thorough discussion. In a justice system with remote hearings, the term "public hearing" requires rethinking. Positions like the one held in Germany will probably be abandoned in the future following the example of countries like the United Kingdom and Norway", where there is live streaming for cases of particular public interest.

Outside Europe, some interesting experiences follow.

In the document entitled "Remote Hearings and Access to Justice. During Covid-19 and Beyond", the National Center for State Courts of the United States,[387] provides these useful guidelines:

- "Security is paramount. Whichever method is proposed, the security of the proceedings is absolutely critical. Issues like "Zoombombing"[388] by members of the public can be disruptive and, at times, indecent or explicit. For this reason, courts should avoid making meetings public if allowed (make private and require password) or sharing the Zoom link or password publicly (such as on a publicly accessible webpage). Also, the court should manage screensharing options so only the "host" (the court) can screenshare and consult the IT department for how to make the meeting as secure as possible (highest Zoom security settings).
- Record the proceedings to provide to the public. The court may also consider providing public access, although not in real time, by posting recordings of the proceedings in the court file for the proceeding, with notice to the public that the recordings are available and how to access them. Non-real time access may be subject to challenge if it is not announced, if content is not complete (absent good cause for confidential proceedings under existing legal standards), or if access is delayed.
- Allow public access through a YouTube channel. If real-time public access is allowed, the court should take reasonable steps to restrict full participation to the parties and court staff. For example, the Zoom platform allows the court to email the link to the Zoom meeting only to those participating in the proceeding, and provide simultaneous access to the public by giving notice of the information necessary to view the proceeding on a YouTube channel that the court can establish."

The US Judicial Information Services has published "Recommendations on using Zoom & Public Access for Court Proceedings", with specific instructions to setup and enable YouTube Live Streaming from a Zoom meeting (initiated/controlled by a Host).[389]

The Superior Court of the District of Columbia provides public access for Remote Court Hearings via a private provider (namely Cisco Webex). To observe the hearing by video, whoever can use the link

[387] https://www.ncsc.org/__data/assets/pdf_file/0018/40365/RRT-Technology-ATJ-Remote-Hearings-Guide.pdf

[388] Zoombombing refers to the unwanted, disruptive intrusion, generally by Internet trolls, into a video-conference call. In a typical Zoombombing incident, a teleconferencing session is hijacked by the insertion of material that is lewd, obscene, racist, misogynistic, homophobic, Islamophobic, or antisemitic in nature, typically resulting in the shutdown of the session. Definition from Wikipedia: https://en.wikipedia.org/wiki/Zoombombing

[389] https://info.courts.mi.gov/virtual-courtroom-info#LiveStreamInfo

provided and enter the generic log in information (First name: Court, Last name: Observer, Email address: obs@trial.crt), so no personal name and email address is needed. The password for criminal jury trials is provided on the website per single hearing.[390] WebEx links to observe all other hearings including civil jury trials are published.[391]

In Canada, namely in Ottawa County, Zoom is used for remote hearings. These are also livestreamed on YouTube, using a Zoom feature.[392]

5.1.2 Guidelines on Videoconferencing

The VC Guidelines deal with this topic in the following points:

- Within the "Guidelines on all judicial proceedings" category, "Right to participate effectively" section, at n. 7 (page 3): "*The court should ensure that the transmission can be seen and heard by those involved in the proceedings and by members of the public where the proceedings are held in public*"
- Within the "Guidelines on all judicial proceedings" category, "Publicity and recording" section, at n. 12 (page 4): "*The court should preserve the public nature of remote hearing by creating a comprehensive procedure for public participation. The publicity of the remote hearing can be ensured, for example, by allowing the public to join the remote hearing in real time or uploading the recordings to the court's website*" N. 13 adds: "*No photographing, recording, broadcasting or any other form of dissemination of any part of the remote hearing (including the audio track) may be made unless previously authorised by the court*"

5.1.3 Current Draft of Law on Digital Efficiency

The current draft contains the following provisions on this sub-topic:

- Title IV, Chapter II, Article 67 (entitled "La emisión de los actos de juicio y vistas telemáticos"):

  Paragraph 1: "*The acts of trial, hearings and other actions that in accordance with the procedural laws are to be practiced in public hearing, when they are held with the telematic participation of all the participants, will be publicly retransmitted in the form established by the State Technical Committee of the Electronic Judicial Administration, provided that the courts, judicial offices and prosecutor offices have the necessary technical means for it*"

  Hence, at this level of legislation no provision on identification/authentication or authorization is indicated for the public.

- Title IV, Chapter III, Article 68 (entitled "Control sobre la difusión de actuaciones telemáticas"):

[390] https://www.dccourts.gov/services/webex-trial-links

[391] https://www.dccourts.gov/sites/default/files/Public-Access-to-Remote-Court-Hearings.pdf

[392] https://www.miottawa.org/Courts/20thCircuit/Virtual_Hearings_Livestream.htm

Paragraph 2: "*In the telematic judicial proceedings described in this title, the parties, interveners or any person who has access to said action, may not record, take images or use any means that allow a subsequent reproduction of the sound and / or the image of what happened*". Sanctions in paragraph 4.

5.1.4 Comments and Recommendations

Public access to a remote hearing can be ensured in two ways: real-time (live) or deferred.

In case of real-time access, there are two options:

a) Through live streaming. Online platforms like YouTube do not request any authentication.

b) Granting access to a videoconferencing platform, which can be a commercial cloud platform (like WebEx, Zoom or Microsoft Teams) or a platform installed and run by the authority/institution (on-premises). Commercial cloud platforms usually provide a link with guest or authenticated access and give the organizer the option to setup a waiting room.

Deferred access means that the public can view and/or listen to a recorded hearing available on a web site. The recording can be available via download or streaming.

With a streaming solution, the content is sent in a continuous stream of data that are played as it arrives. Users can pause, rewind or fast-forward, just as they could do with a downloaded file (unless the content is being streamed live).

Live broadcast allows content distributors to monitor what visitors are watching and how long they are watching it. It provides an efficient use of bandwidth because only the part of the file being transferred is the part being watched. Streaming media has also the benefit of providing the content creator with more control over his intellectual property because the video file is not stored on the viewer's computer. Once the video data has been played, it is discarded by the media player.

The current draft of the Law does not indicate the form of the retransmission, if it is going to be real-time or deferred, leaving the decision to a secondary level of legislation established by the State Technical Committee of the Electronic Judicial Administration. We believe this is a correct approach, considering the strong dependencies on the technical choices – both on hardware and software – that are subject to constant evolution, and on the budget available (e.g., on devices, licenses, and network bandwidth).

According to the VC Guidelines, a comprehensive procedure for public participation should be created: following the best practices mentioned above, we believe it is necessary to provide exhaustive and easy-to-reach information on all involved web sites, starting with the new "General Access Point of the Administration of Justice", as foreseen in Article 12 of the current draft of the Law.

In case real-time access is provided, and a videoconferencing platform is used (instead of live streaming system, so like WebEx, Zoom or Microsoft Teams), published information should contain clear instructions on how to join the virtual room, if there is a waiting room, etc.

Furthermore, in case the platform provides the related features, having a public frontstage and a backstage with private facilities, to which the public has no access, is preferable. Please refer to the aforementioned experimental virtual jury trials that took place in England for more details. It is undoubtful that in order to manage different stages, as well as to control microphones, update indications for the public, etc., adequately trained operators are required, being them on-site or in a centralized control-room.

Quality and availability of the overall technical means, being them devices (cameras, microphones), software platform or connectivity, are not minor issues, considering the need to ensure that all the parties can see each other's faces very clearly and were accorded equal visual status. In the view of the authors of the article on the English pilot study, this constituted a success for open justice.[393]

Article 68 of the Law of Digital Efficiency explicitly prohibits to record, take images or use any means that allow a subsequent reproduction of the sound and/or the image. It has to be pointed out that it is not currently technically possible to detect the use of recording software on the remotely connected computer.

5.2 Security of Remote Witnesses

5.2.1 Information from Other Countries

On this topic, the Survey asked if there is national legislation (in force or under preparation) or best practices that cover the following aspects related to remote court hearings:

- Participation to court proceedings by parties or witnesses via videoconferencing from home or another place of their choice. (ref. Item 2.1 of the Survey)
- If the reply to the above question is "Yes", is there a procedure to formally identify the participants during the proceedings? (ref. Item 2.2 of the Survey)
- Participation to court proceedings via videoconferencing from the premises of a court different from the one which is handling the case, or from other protected locations. (ref. Item 2.3 of the Survey)
- Measures to ensure the security and privacy of victims and witnesses, such as secured spaces, voice distortion, picture blur/distortion, etc. (ref. Item 2.7 of the Survey).

The following tables summarizes the answers provided:

[393] "Exploring the Case for Virtual Jury Trials during the COVID-19 Crisis: An Evaluation of a Pilot Study Conducted by JUSTICE", page 22: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3876199_code3690616.pdf?abstractid=3876199&mirid=1

Country	2.1	2.2	2.3	2.7	Comment (to specific topic)
Cyprus	No	No	**Yes**	No	In criminal cases, witnesses from abroad, are able to give testimony via videoconferencing.[394]
Austria	**Yes**	No	**Yes**	No	-
Ireland	**Yes**	**Yes**	**Yes**	**Yes**	-
Suisse	**Yes**	**Yes**	**Yes**	**Yes**	[translated from French] Current legislation only authorizes the use of videoconferencing in criminal proceedings.
North Macedonia	**Yes**	**Yes**	**Yes**	**Yes**	There is no legislation yet, but it is in the phase of preparation, so all answers are Yes. All above mentioned issues are going to be included in the Law on criminal procedure and in the Judicial rules of procedure.
Slovakia (Ministry of Justice)	No	No	No	No	There are some minor projects in specific court agendas, where MOJ with the courts is testing the possibility doing remote court hearings
Luxembourg	No	No	**Yes**	No	Remote hearings are possible under covid legislation for pretrial hearings of persons in prison. This possibility is foreseen by law to end of 2021
Germany	**Yes**	No	**Yes**	**Yes**	(2.1) The legal regime for remote hearings varies between the different branches of the judiciary. (2.2) There is no formal or general procedure for the identification of participants. It is up to the court in session to set the requirements in each concrete case
Monaco	**Yes**	No	**Yes**	No	-
Bosnia and Herzegovina	**Yes**	**Yes**	**Yes**	**Yes**	-
Sweden	**Yes**	No	**Yes**	**Yes**	-
Norway	**Yes**	No	**Yes**	**Yes**	-
Latvia	**Yes**	**Yes**	**Yes**	No	-
Lithuania	**Yes**	**Yes**	No	**Yes**	-
Slovakia (IT project manager)	No	No	**Yes**	**Yes**	-

[394] Relevant Legislation: http://www.cylaw.org/nomoi/indexes/2004_3_25.html

The Netherlands	**Yes**	**Yes**	**Yes**	**Yes**	Online court proceedings in the Netherlands take place in all areas of law, but particularly in administrative and civil law cases. Participation in such hearings by request. In criminal law cases court hearings ('telehoren') can be arranged in some cases, with no option to remotely access the hearings.
Ukraine	**Yes**	**Yes**	**Yes**	No	-
Slovenia	**Yes**	No	**Yes**	**Yes**	-
France	No	No	**Yes**	No	Ex: article 706-71 for criminal matters: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042779899/

Upon direct request to the contact points that provided the answers, some clarifications follow:

- Latvia: The mechanisms for verifying identity are several and the court chooses the appropriate option. One of the options is to show the ID, passport or to scan/photograph the passport and to send it to the court and to certify the identity during the hearing. The courts also have access to the Citizenship and Migration Affairs Management System, where they can check ID documents, and they can also see a picture on the document to make sure that the person on the screen corresponds to the ID. It is also possible to produce a personal identification document by means of a video camera, or the person directing the process can verify the identity of the person after photocopies of the documents submitted to the person directing the proceedings. The practice of the prosecutor's office also includes cases where e-signature and www.latvija.lv tools were used to verify the identity of the person. A member may also sign a statement prior to the meeting with his e-signature of participation in the meeting, thereby confirming his identity.[395]
- Sweden: For a person who is threatened and lives at a secret location, only audio is active during a videoconference, and the place is kept secret for everyone in the courtroom, not even the court staff will know. The court clerk will be given a number to use in the video conference system that connects to another court or a police station, somewhere in Sweden, where the victim or witness is situated. There is no specific legislation about this situation. Furthermore, there are no provisions in Swedish law to keep a witness identity secret (like blurred picture or distorted voice), since anonymous witnesses are not allowed in Sweden, with the very rare exception of police witnesses who can sometimes testify under a false name in order not to sabotage their future work.
- Switzerland: In criminal proceedings the identification is done by an employee of the prison when the parties are in prison; in civil and administrative proceedings, the identification is done after a presentation of an identity card and questions asked by the court's president. There is no specific

[395] For example, see Criminal Procedure Law, Section 140, and further sections.

regulation regarding the identification of parties or witnesses. The following protective measures apply as per Swiss Criminal Procedure Code:[396]

Art. 149 General provisions

1. *If there are grounds to assume that a witness, a person providing information, an accused person, an expert witness or a translator or interpreter, or a person related to him or her in terms of Article 168 paragraphs 1–3 could be exposed to a serious danger to life and limb or any other serious prejudice by participating in the proceedings, the director of proceedings shall take the appropriate protective measures in response to an application or ex officio.*
2. *The director of proceedings may also suitably restrict the procedural rights of the parties, in particular by:*
    a. *ensuring anonymity;*
    b. *conducting examination hearings while excluding parties or the public;*
    c. *establishing personal details while excluding parties or the public;*
    d. *modifying the appearance or voice of the person requiring protection or screening the person from the court;*
    e. *limiting rights to inspect case documents.*
3. *The director of proceedings may permit the person requiring protection to be accompanied by a legal agent or a confidant.*
4. *If a person under the age of 18 is interviewed as a witness or person providing information, the director of proceedings may order further protective measures in accordance with Article 154 paragraphs 2 and 4.*
5. *The director of proceedings shall ensure in the case of all protective measures that the right of the parties to be heard is respected and in particular that the accused's rights to a proper defence are respected.*
6. *If the person requiring protection has been assured that his or her anonymity will be preserved, the director of proceedings shall take appropriate measures to prevent any confusion or mistaken identity.*

Art. 150 Assurance of anonymity

1. *The director of proceedings may give an assurance to the person requiring protection that his or her anonymity will be preserved.*
2. *The public prosecutor shall submit its assurance to the compulsory measures court within 30 days for approval; in doing so, it must specify all the details required to assess the legality of the measure. The decision of the compulsory measures court is final.*
3. *If the compulsory measures court declines to approve the measure, any evidence already obtained subject to the assurance of anonymity shall be inadmissible.*

[396] Section 4: https://www.fedlex.admin.ch/eli/cc/2010/267/en#tit_4/chap_1/sec_4

4. *An assurance of anonymity that has been approved or granted is binding on all criminal justice authorities involved in the case.*
5. *The person requiring protection may waive the requirement of anonymity at any time.*
6. *The public prosecutor and the director of proceedings in the court shall revoke the assurance if there is clearly no longer a need for protection.*

There are also measures to protect undercover investigators and victims (general and special for some kinds of victims).

As per direct knowledge of one of the experts, as said, in Italy criminal trials that take place in videoconference require that the judges, the prosecutors and the lawyers are physically present in the courtroom. Defendants are connected from equipped rooms in prisons. Every room is indicated on the screen with a code that also contains the abbreviation of the location. Witnesses can be connected from different places, either another courtroom or in one equipped penitentiary establishment. In case the witness' location is to be kept confidential, to protect the person, the indication of the screen is not provided. No voice distortion or picture blur/distortion is in place. It must be pointed out that the Italian system has a central control room where an adequate number of operators and experts are able to remotely control all involved devices (cameras, microphones, speakers) during the sessions, as well as what is seen on the screens: when there are protected witnesses, the control room is previously informed in order to put in place the specific setup required.

In England, in order to provide security for the witness in court proceedings where the public is enabled to see and hear remote hearings, two special sections were introduced in Courts Act 2003 to deal with offences of unauthorised recording or transmission of broadcasted or online transmitted hearings:

- Section 85B dealing with offences of recording or transmission in relation to broadcasted hearings,[397] and
- Section 85C dealing with offences of recording or transmitting participation through live link.[398]

These rules concern images and sound material that are recorded or transmitted without the authorisation of the court as well as any attempt made to record or transmit such materials. The person found guilty of contempt of court due to recording or transmitting broadcasted proceedings offence will be liable on summary conviction to a fine. A similar conviction is to be handed in relation to recording or transmission of proceedings in which a person participates via a live link. It does not matter if this attempt or recording is made for itself or for being seen or heard by other persons.

The effect of these provisions was considered by the High Court in the case of *R (Good Law Project and others) v Secretary of State for Health and Social Care* [2021].[399] In this case the court interpreted

[397] Rules are available at https://www.legislation.gov.uk/ukpga/2003/39/section/85B.

[398] Rules are available at https://www.legislation.gov.uk/ukpga/2003/39/section/85C.

[399] R (Good Law Project and others) v Secretary of State for Health and Social Care [2021] EWHC 346 (Admin), see para. 162-168. The case is available at https://www.bailii.org/ew/cases/EWHC/Admin/2021/346.html.

Section 85A as allowing the court to authorise a hearing to be recorded for the court's own records, or to be broadcast live to the public, but not for it to be both recorded and then broadcast it to the public in the form of a catch-up video.[400]

To sensitise members of the public on the consequences of transmission and recording of transmission of materials from court proceedings taking place online the attorney general has launched a campaign warning of the legal consequences of prejudicing the judicial process via social media.[401] In this he underlines the importance of ensuring fair trials and fair treatment for defendants, victims and witnesses. In order to reach out he uses simple examples of situations in online court proceedings to educate the public and journalists and provide guidance on how to avoid committing a contempt of court when posting information online on social media about court proceedings.[402]

An interesting practice can be found in Poland:[403] A "lobby" function is used in the Court of Appeal in Wrocław (Poland) during the examination of the witnesses. The court is working on modification of the platform to transform the standard "lobby" function into a full "waiting room" functionality adapting it to the needs of the courts and allowing for personalised links for participants and efficient communication also outside the videoconferencing rooms, e.g., to inform about the possible delay of the proceedings.

5.2.2 Guidelines on Videoconferencing

The VC Guidelines deal with this topic in the following points:

- Within the "Guidelines on all judicial proceedings" category, "Witnesses and experts" section, at n. 14 (page 4): "*As far as a national legal system permits, the examination of the witnesses and experts during the remote hearing should follow as closely as possible the practice adopted when a witness or expert is present in the courtroom*". N. 15 adds: "*The respective arrangements should be given special consideration in order to ensure the integrity of remote hearings and avoid pressure or influence on the witnesses or experts during such hearings*"
- Within the "Guidelines specifically for criminal proceedings", "Legitimate aim" section, at n. 22 (page 4): "*The legitimate aim of remote hearing in criminal proceedings should be based on such values as the […] security of witnesses and victims of crimes*"

[400] For further comments see Paul Magrath, The PPE procurement case: transparency missed in both politics and law, 23 February 2021 (available at The PPE procurement case: transparency missed in both politics and law | The Transparency Project); Judith Townend & Paul Magrath (2021), "Remote trial and error: how COVID-19 changed public access to court proceedings", Journal of Media Law, https://doi.org/10.1080/17577632.2021.1979844

[401] https://www.gov.uk/government/news/attorney-general-launches-new-campaign-to-combat-contempt-of-court-online.

[402] Such examples can be consulted https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/996664/Contempt_of_court_and_social_media_case_studies.pdf.

[403] From a document dated 30/11/2021 and entitled "Selected national good practices on videoconferencing in judicial proceedings - Complement to the CEPEJ Guidelines on videoconferencing in judicial proceedings", prepared by Marek Świerczyński and Alexandre Palanco

- In the appendix "Checklist for conducting videoconferences in judicial practice", three items are indicated regarding witness protection:
  - separate witness rooms (possible off-site)
  - voice distortion
  - picture blur/distortion/deactivation.

5.2.3 Current Draft of Law on digital efficiency

- Title IV, Chapter I, Article 61 (entitled "Regla general de identificación y firma"):

  Paragraph 3: "*The provisions of the preceding paragraphs* [related to the need to identify participants at the beginning of the hearing] *may be exempted in the case of protected witnesses or experts, police officers, undercover police officers, and, ultimately, in the case of any person whose identity must be preserved in the process, in accordance with the law.*"

  Paragraph 5: "*Systems or applications that alter or distort the image and sound transmitted may not be used in the intervention by videoconference, except relating to the safeguarding of identity in the cases provided for in paragraph 3 of this Article*"

- Title IV, Chapter II, Article 67 (entitled "La emisión de los actos de juicio y vistas telemáticos"):

  Paragraph 3: "*Likewise, in the criminal field, in accordance with article 682 of the Code of Criminal Procedure, the judge or court, after hearing the parties, may restrict the presence of the audiovisual media in the sessions of the trial and establish limitations on recordings and taking of images, to the publicity of information on the identity of the victims, of witnesses or experts or of any other person involved in the trial.*"

5.2.4 Comments and recommendations

We believe that the current draft of Law on digital efficiency already covers the necessary provisions at the first level of legislation regarding witness protection.

On a more practical level, the videoconferencing system should provide the possibility for a trained operator (in the courtroom or from the control room) to quickly configure the session in order to set the voice distortion, picture blur/distortion/deactivation, or simply to move the camera to change the view.

The "lobby" function used in the Court of Appeal in Wrocław (Poland) should also be considered as a useful solution.

5.3 Legal Validity in Case of Exception or Appeal

5.3.1 Information from Other Countries

On this topic, the survey asked if there are methods to check the legal validity in case of exceptions being raised or appeals, for example the supplying of technical info, logs, etc. that could prove the quality of the systems, eventual incidents, etc. (ref. Item 2.8 of the survey).

The following tables summarizes the answers provided:

Country	2.8
Cyprus	No
Austria	No
Ireland	**Yes**
Suisse	No
North Macedonia	**Yes**
Slovakia (Ministry of Justice)	No
Luxembourg	No
Germany	No
Monaco	No
Bosnia and Herzegovina	No
Sweden	No
Norway	No
Latvia	**Yes**
Lithuania	**Yes**
Slovakia (IT project manager)	No
The Netherlands	**Yes**
Ukraine	No
Slovenia	**Yes**
France	No

No comments were provided for this specific topic.

In Italy, the system for videoconference in criminal cases adopts the following measures:

- About 30 minutes before the hearing, the audio and video quality is tested with the operator of the control room assigned to the session.
- The operator of the control room monitors the quality during the session.
- The control room acts like a help desk in case of problems and immediately intervenes.
- The system is installed in two data centres in order to ensure redundancy: in case of fail-over of one data centre, the other one steps in immediately.

- The system runs on a dedicated virtual private network over the Intranet of the Ministry of Justice, so it's protected from intrusions. An adequate bandwidth is dedicated to the network in order to ensure quality persistence.
- The system is setup in a way that all sessions are recorded, and any event is logged. Recordings and logs are kept for a certain period of time. This enables to provide specific information upon request.

The President of the Italian State Council has established by decree that the lawyers, or the parties acting on their own, guarantee the correct functionality of the device used to connect to the videoconference, the updating of its basic and application software to the most recent versions made available by the respective manufacturers (or support communities in the case of open source software) with particular reference to the installation of all updates and corrections relating to IT security, and the use of a suitable and updated antivirus program.[404]

In the Netherlands, it is expected that limitations related to the quality of the online connection of a remote hearing and complains in this regard will be dealt with by the courts organising the hearing or the complaints boards.[405] Available case law related to remote hearings in the Netherlands addressed the question whether a digital hearing fulfils the requirements of the right to an oral hearing, as protected by Article 6 ECHR. Technical aspects such as the quality of the connection during the remote court hearing was only indirectly touched upon because they were not part of the grounds of appeal raised by the party. The decision concerned a criminal case handled by the time during COVID-19 restriction period when in person hearings were not held and the court carried this out by telephone and not via a video link.[406] The Supreme Court (*Hoge Raad*) ruled that the telephone connection was "the only option available at that time" and that the physical presence of a suspect at the hearing is a starting point, but not an absolute requirement (paragraphs 3.2.3-3.2.4 of the decision). The court recognised that the factual circumstances were taken into account including the safety measures imposed by the law to ensure the observance of the requirements of Article 6 ECHR and that "technical problems must not stand in the way of effective participation in the session" (paragraph 3.2.4). Thus, if the physical presence of the person concerned at the hearing is not reasonably possible or not justified in the circumstances of the case, the Court established that "a different form of participation in the hearing can be chosen, which in principle includes participation by means of a two-way video and audio connection. It can be assumed that, if such a connection is not possible, in urgent cases it is possible to opt for a telephone handling of the case" (paragraph 3.2.5).

[404] Art 2 paragraph 6 of decree n. 134/2020 del Presidente Consiglio di Stato

[405] Bart Krans (2020), "The Aftermath of the COVID-19 Pandemic in The Netherlands. Seizing the Digital Gains", in Bart Krans and Anna Nylund (eds.) *Civil Courts Coping with COVID-19*, Eleven International Publishing, p. 133.

[406] HR (Supreme Court) 25 September 2020, ECLI:NL:2020:1509, sub 3.2.1-3.2.5 (available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2020:1509).

The Australian Guide on Videoconferencing in the Federal Court[407] reminds that participants should remain alert to any deterioration in picture and sound quality and inform the judicial officer immediately if this is impacting on their ability to participate fully.

5.3.2 Guidelines on Videoconferencing

The Guidelines on Videoconferencing do not specifically deal with this topic. It could be useful, though, to quote the points under the "Right to participate effectively" section in page 3, i.e.:

- At n. 5: "*The court should give the participants the opportunity to test the audio and video quality, either prior, for example through self-testing, or at the start of the hearing allowing each participant to familiarise themselves with the features of the videoconferencing platform*"
- At n. 6: "*During the remote hearing, the court should be able to continuously monitor the quality of the image and sound of the video link in order to minimize technical incidents that may affect the right of the parties to participate effectively in the proceedings*"
- At. n. 7: "*The court should ensure that the transmission can be seen and heard by those involved in the proceedings*"
- At. n. 8: "*The court should consider the situation and challenges of persons in vulnerable positions, such as children, migrants, or persons with disabilities in the decision to have a remote hearing and its modalities*"
- At n. 9: "*The court should suspend the hearing in case of a technical incident until it has been corrected, depending on its nature. Such a suspension should be registered in the minutes of the remote hearing*".

Other points to be considered from the guidelines are the following on security and technical standards:

- At n. 42 (page 6): "*Practical arrangements should be made in advance to mitigate the risk that the videoconferencing hardware, software and connections are vulnerable to improper access, such as hacking or other illicit access*"
- At n. 43 (page 6): "*Contingency plans should be in place in order to effectively deal with issues such as sudden technical failures, disconnections, power outages (alternative communication channels and technical support), or data security breaches*"
- At n. 50 (page 7): "*The videoconferencing hardware and software should provide video and audio of sufficient quality to hold continuous and adequate audio-visual connectivity, enabling parties to follow the proceedings and effectively participate in them*"

[407] https://www.fedcourt.gov.au/going-to-court/videoconferencing-guide

– At n. 51 (page 7): "*All participants to the remote hearing, in particular the judge, should be able to see and hear both the speaker asking questions or making statements when heard, and the reaction of the other participants*".

Regarding guideline 42, the following good practice is indicated:[408] Finnish Guide on the use of remote access in court dated 15 April 2020 points out that attention must be paid to the security of the selected remote access platform. When making a choice between different remote access methods (video, telephone, etc.), the court should decide on the suitability of the chosen solution for the specific case. The assessment of the risks associated with the chosen remote access method is required. The following example is provided in the Finnish Guide: A criminal case concerns breach of a trade secret involving confidential information relating to the activities of a company. The judge is considering the use of Skype for a court session, whose functional characteristics are considered by the judge and the parties as suitable for the trial. Nevertheless, further consideration is needed whether there is a risk that, for example, the Skype link will be disclosed to third parties or that such other person could participate in the Skype meeting which may compromise the confidential information.

5.3.3 Current Draft of Law on digital efficiency

Title IV, Chapter III, Article 68 (entitled "Control sobre la difusión de actuaciones telemáticas"):

> Paragraph 3: "*Recordings to which any person has had access in connection with a judicial proceeding may not be used, without judicial authorisation, for purposes other than jurisdictional ones.*".

5.3.4 Comments and Recommendations

Following the videoconferencing guidelines mentioned above, a secondary legislation – or at least practical guidelines – should discipline the following measures:

– an organization measure to give the participants the opportunity to test the audio and video quality in due time before the start of the hearing, also in order to allow them to familiarise with the platform

– technical requirements for adequate devices and upgraded software used by external users (lawyers, parties, experts, etc.)

– technical and organization measures to continuously monitor the quality of the image and sound during the hearing and to ensure that everyone can see and hear, combining automated monitoring features of the platform with human control; participants should be provided with contact details to request assistance

– procedural indications on how to manage the suspension of the hearing in case of a technical incident until it has been corrected, depending on its nature, like registering it in the minutes.

[408] Op.cit. "Selected national good practices on videoconferencing in judicial proceedings - Complement to the CEPEJ Guidelines on videoconferencing in judicial proceedings", p. 7.

We also suggest that the videoconferencing platform fulfils the following requirements:

- Provide an adequate logging subsystem, which automatically records all significant events (start, end, pauses, etc.), including issues (failures, disconnections, etc.).
- Logs should be archived in such a way to guarantee integrity and long-time preservation; for this purpose, a log management platform is suggested.
- Ensure high availability, through redundancy and the implementation of a business continuity plan.
- Guarantee an adequate bandwidth dedicated to the videoconference VC service over the network.
- Be adequately protected from cyberattacks, undergoing periodic vulnerability tests, especially in case the system is connected to the internet.