European Economic and Social Committee

OPINION

European Economic and Social Committee

Digitalisation of cross-border judicial cooperation

Proposal for a regulation of the European Parliament and of the Council on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation
[COM(2021) 759 final – 2021/0394 (COD)]

Proposal for a Directive of the European Parliament and of the Council amending Council Directive 2003/8/EC, Council Framework Decisions 2002/465/JHA, 2002/584/JHA, 2003/577/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA, 2008/947/JHA, 2009/829/JHA and 2009/948/JHA, and Directive 2014/41/EU of the European Parliament and of the Council, as regards digitalisation of judicial cooperation
[COM(2021) 760 final - 2021/0395 (COD)]

SOC/711

Rapporteur: **Maurizio MENSI**

www.eesc.europa.eu

EN

www.eesc.europa.eu/facebook www.eesc.europa.eu/twitter www.eesc.europa.eu/linkedin www.eesc.europa.eu/instagram

Referral	European Commission, 02/05/2022
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Employment, Social Affairs and Citizenship
Adopted in section	03/05/2022
Adopted at plenary	19/05/2022
Plenary session No	569
Outcome of vote (for/against/abstentions)	198/0/1

1. Conclusions and recommendations

1.1 The EESC supports the Commission's approach and the objectives pursued through this proposal for a regulation. However, believes that adequate safeguards in the following areas need to be provided: a) security and confidentiality, given the sensitive nature of the issues covered in the various hearings; b) open justice, that is to say, the system envisaged must ensure compliance with the open justice principle in terms of participation, observation and accessibility; and c) digital divide, in order to ensure accessibility for all in terms of support measures and technologies. This is to prevent poor digital skills, limited access to technology, and low levels of literacy and legal knowledge increasing the barriers to accessing digital services and thwarting the stated aims.

1.2 It is essential to ensure the security of the technological systems used and the confidentiality of the data involved – especially personal data – given the sensitive nature of certain types of court hearings. It is also fundamental that the online platform to be used be accurately assessed.

1.3 It must also be ensured that no data be processed by the entity in charge of the operational management of the system components, and that an adequate bandwidth be available, since the slightest interruption or inconsistency could hinder the system's ability to provide an adequate service.

1.4 It is essential that systems, networks and data be adequately protected against possible cyber-attacks, guaranteeing the integrity of the data they carry and store, on the basis of current data protection and cybersecurity rules. The IT systems and digital communication technology in question must also be accessible in accordance with the requirements of the European Accessibility Directive and the Directive on the accessibility of the websites of public administrations, and in accordance with the United Nations Convention on the Rights of Persons with Disabilities of 13 December 2006.

1.5 The system envisaged must ensure compliance with the open justice principle (in terms of participation, observation and accessibility) in relation to access to the justice system in general, and with specific regard to public hearings. Accessibility for all must therefore be ensured, in terms of support measures and technology.

1.6 It is essential that natural and legal persons retain the option of using paper-based communication channels, and that information is provided in an accessible format in order to ensure access to justice for all, including vulnerable people, minors, and those in need of technical assistance, who live in remote areas, or who otherwise do not have access to digital means or possess the necessary skills.

1.7 Training legal practitioners in Union law is an essential tool for ensuring the correct and effective application of the regulation. This requires organising timely and targeted training activities for all legal practitioners involved in the activities envisaged under the proposed regulation. In particular, specific training focused on the needs of suspects, the accused, witnesses or vulnerable victims is necessary, in order to ensure proper access to justice via digital means.

1.8 In essence, the proposed measures seem likely to improve the efficiency of the judicial system by reducing and simplifying administrative burdens, reducing the time and cost of dealing with cases, and must result in a better and more equal access to justice. In this regard, the EESC believes that, subject to the above, the proposed measures benefit cross-border trade and the competitiveness of the European economic and social system.

2. General comments

2.1 Content of the Regulation

2.1.1 The proposed regulation establishes the legal framework for electronic communication in the context of procedures for cross-border judicial cooperation in civil, commercial and criminal matters, and access to justice in civil and commercial matters with cross-border implications, as provided for under existing law.

2.1.2 It also lays down rules on the use and recognition of electronic trust services, on the legal effects of electronic documents, and on the use of videoconferencing or other accessible distance communication technology for the hearings of persons in civil, commercial and criminal matters. However, the regulation does not cover the procedure for the taking of evidence in civil and commercial matters, and does not introduce new procedures.

2.1.3 In order to be secure and reliable, it is based on a decentralised IT system consisting of interoperable IT systems and access points operating under the responsibility and management of each Member State and of EU agencies and bodies, through which cross-border exchanges between the respective authorities of the Member States take place.

2.1.4 A European electronic access point is envisaged for the European e-justice portal, which is part of this decentralised IT system, and which may be used under the same conditions by all natural and legal persons for electronic communications with courts and competent authorities in civil and commercial matters with cross-border implications.

2.1.5 Member State courts and competent authorities will therefore be obliged to accept electronic communications in judicial proceedings, which are considered equivalent to paper communications. However, natural persons are free to opt for electronic or paper-based means of communication, which cannot be rejected by the competent authorities.

2.1.6 The regulation also lays down conditions for the use of videoconferencing or other distance communication technology in cross-border civil and commercial proceedings. Furthermore, it lays down rules on the hearings of a suspect, accused or convicted person and of minors by videoconference or other distance communication technology.

2.2 **Background**

2.2.1 The legislative initiative is based on the premise that natural and legal persons should be able to exercise their rights and comply with their obligations in a swift, cost-efficient and transparent manner, free from discrimination of any kind. Obtaining effective access to justice within a reasonable time is also a crucial aspect of the right to a fair trial, enshrined in Article 47 of the Charter of Fundamental Rights of the European Union[1].

2.2.2 A number of instruments already exist at EU level to strengthen judicial cooperation and access to justice in cross-border civil, commercial and criminal matters. These include instruments relating to communication between authorities, and, in certain cases, communications with EU agencies and bodies dealing with Justice and Home Affairs (JHA) . However, most of these instruments do not provide for the use of digital communications and, even where they do, there remains a lack of secure and reliable channels, or the non-recognition of electronic documents, signatures and seals.

2.2.3 The health emergency has also shown that events of *force majeure* affect and have an impact on the normal functioning of Member States' judicial systems due to the total lockdown of the population in such cases. Judicial cooperation and access to justice in cross-border disputes in the EU have also been affected by the health emergency, which has highlighted the need to ensure secure, continuous and resilient communication, also to avoid disrupting the smooth running of economic activities.

2.2.4 In this respect, the rules in the proposal aim to improve both access to justice under the same conditions, and the efficiency and resilience of communication flows related to EU judicial cooperation. The use of digital technologies eases the administrative burden on judicial systems by shortening case-handling times, making communications more secure and reliable, and automating case management.

2.2.5 The Commission's initiative also stems from the need to avoid the development of IT solutions at national level leading to fragmented solutions that are not compatible with the need to ensure uniform action at EU level.

2.2.6 The proposal for a regulation was preceded by the Communication on the digitisation of justice in the EU of December 2020, which modernises the legal framework on EU cross-border procedures in civil, commercial and criminal law, in line with the 'digital by default' principle, recognising the need to avoid all forms of social exclusion. This proposal comes on top of the proposal for a regulation on a computerised communication system for cross-border civil and criminal proceedings (the 'e-CODEX' system)[2], and is consistent with the eIDAS regulation[3] as it introduces provisions on the use of trust services. In June 2021, the Commission also adopted

1 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391

2 COM(2020) 712 final.

3 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

a proposal amending the eIDAS Regulation to establish a framework for a European digital identity[4].

2.3 Specific comments

2.3.1 The EESC supports the Commission's approach and objectives. However, the EESC deems it essential that the following points be safeguarded.

2.4 Data processing and cybersecurity

2.4.1 The implementation of the Regulation entails establishing and maintaining a decentralised IT system consisting of a network of national IT systems and interoperable access points operating under the responsibility and management of each Member State, EU institution or agency, for the secure and reliable exchange of information across borders. It is important to ensure that the data are not stored or processed by the entity in charge of the operational management of the system components, and that the hardware used is able to support the IT system. The EESC welcomes the provision whereby the Commission will provide reference implementation software that Member States may choose to use, where Member States have not already developed appropriate national IT systems.

2.4.2 The availability of adequate bandwidth (an expensive component of video link services) is important. The recommended bandwidth is at least 1.5-2 megabits per second for IP networks (or at least 384 kilobits per second for ISDN networks). Video link systems should be designed with the highest possible bandwidth capacity, and even for systems with the highest capacity, consideration should be given to the reliability and performance of the network connection, as the slightest interruption or inconsistency may hinder the system's ability to provide a good service.

2.4.3 The EESC therefore points to the need to ensure technical standards for the digital communication used, and to protect systems, networks and data from cyber-attacks, bearing in mind that the two systems have completely different paper-based and digital vulnerabilities, and thus systems and networks must be protected by guaranteeing the integrity of the data they carry and store, on the basis of current data protection rules. The IT systems and digital communication technology in question must also be accessible in accordance with the requirements of the European Accessibility Directive[5], and the Directive on the accessibility of the websites of public administrations and companies of public interest[6].

4 COM(2021) 281 final.

5 Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

6 Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1).

2.4.4 As already pointed out by the EESC in its opinion SOC/573, *Interoperability package*, of 23 May 2018[7], given the sensitive nature of the information exchanged, it is essential to ensure both compliance with data protection rules and the security of the data and systems involved.

2.4.5 Video transmissions in both criminal proceedings and in civil and commercial matters should be secured against unlawful interception by third parties, using technical means proportionate to the case. In this regard, compliance should be ensured with both the existing cybersecurity rules and the content of the proposed NIS 2 directive[8].

2.5 Training

2.5.1 The EESC emphasises that training legal practitioners in Union law is an essential tool for ensuring the correct and effective application of the regulation. In order to prepare legal practitioners for future challenges, the Commission has adopted a European judicial training strategy for 2021-2024[9] to train them in the use of digital tools in their daily work. To this end, it is essential to organise timely and targeted training activities for all legal practitioners involved in the activities envisaged under the proposed regulation.

2.5.2 In particular, specific training focused on the needs of suspects, the accused, witnesses or vulnerable victims is necessary, in order to ensure that they have proper access to justice via digital means.

2.6 Digital and paper-based tools

2.6.1 The proposed regulation aims to enable natural and legal persons to communicate with the courts and competent authorities via digital means, free from discrimination of any kind, and take part in hearings via videoconference or other accessible distance communication technology without any specific additional costs beyond those for computer use and access to the internet.

2.6.2 The EESC considers it essential that natural and legal persons retain the option of using paper-based communication channels, and that information is provided in accessible formats in order to ensure access to justice for all, including vulnerable people, minors, and those in need of technical assistance, who live in remote areas, or who otherwise do not have access to digital means or possess the necessary skills.

2.6.3 With specific reference to videoconferencing, which has been systematically introduced in many countries and which is also used for judicial cooperation, it should be noted that according

---

7 Opinion of the European Economic and Social Committee SOC/573 OJ C 283, 10.8.2018, p. 48 on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 (COM(2017) 793 final – 2017/0351 (COD)) – Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) (COM(2017) 794 final – 2017/0352 (COD)).

8 COM(2020) 823 final.

9 COM(2020) 713 final.

to the European Court of Human Rights, although it is not contrary to the Convention for defendants to participate in proceedings via videoconference, its use must have a legitimate purpose[10]. Courts using videoconferencing should therefore continue to improve the quality of videoconferencing and apply video signal encryption to avoid eavesdropping. In its opinion (2011)14 on *justice and information technologies (IT)*, the Consultative Council of European Judges (CCJE) stresses that the introduction of IT in courts in Europe should not compromise the human and symbolic faces of justice. If justice is perceived by users as being purely technical, without performing its real and fundamental function, it risks being dehumanised.

2.6.4 In the United States, video links are mainly used for what are called 'bail hearings' to save costs and avoid the risks of transporting defendants from prison to court. Researchers at Northwestern University studied the amount of bail money set before and after the advent of videos, and concluded that videoconferencing increased bail amounts by an average of 51%[11]. Video transmission actually has a dehumanising effect, and puts defendants at a visual and auditory disadvantage. In immigration hearings, if people appear on video, they are more likely to be deported than if they appear in person, and the same is true for asylum seekers. What people in court can see and hear is also important. The audio function of some videoconferencing technologies uses a medium bandwidth filter that cuts off low- and high-voice frequencies, which are typically used to convey emotion, as detailed in a 2015 US Department of Justice-funded report on video hearings.

2.6.5 Regarding the software used, it should be noted that the availability of open-source software solutions that are comparable in reliability and accuracy to the best industrial products offers the advantage of allowing direct 'implementation' on data centres and networks or on infrastructure collectively managed by or with the public administration. This solution would avoid the risks of cross-border flows within or outside the EU linked to cloud solutions of non-European companies (thus avoiding the application of the US Cloud Act).

2.7 **Improving efficiency and competitiveness**

2.7.1 The EESC agrees with the Commission that the use of digital communication tools between courts and competent authorities in Member States can undoubtedly contribute to greater efficiency in the judicial system, as it is intended to reduce delays and administrative burdens, simplifying and speeding up the exchange of information between authorities, and reducing the time taken to process cases, as well as related costs. It should be noted that distance communication during the health emergency has made it possible to continue ensuring access to justice, helping to guarantee its quality, efficiency and independence, which are essential elements underpinning the rule of law and the values on which the European Union is founded.

2.7.2 The EESC also believes that having efficient judicial systems is fundamental for implementing European law, as highlighted in the European Commission's communication on the *EU Justice Scoreboard 2019* of 26 April 2019, which provides an annual overview of indicators relevant to

10 Judgement of the European Court of Human Rights of 5 October 2006, *Marcello Viola vs. Italy*. Right to a fair trial - Importance of the defendant's presence in the proceedings.

11 Kirchner, L., 'How fair is Zoom-Justice?', *The Markup*, 9 June 2020.

the independence, quality and efficiency of judicial systems, based on data from the Council of Europe's Commission for the Evaluation of the Efficiency of Justice (CEPEJ).

2.7.3 As such, the possibility for natural and legal persons involved in cross-border operations to benefit from better and more equal access to justice, lower costs, and faster procedures for enforcing their rights will bring benefits for cross-border trade, and generally improve the competitiveness of the economic system.

2.8 In conclusion, the EESC notes that the proposal should provide adequate safeguards with respect to the following:

a) Security of the technology used: security and confidentiality are crucial, given the sensitive nature of some court hearings. It is also essential that IT experts carefully assess the online platforms used.
b) Open justice: the system envisaged must ensure compliance with the open justice principle (in terms of participation, observation and accessibility).
c) Digital divide: poor digital skills, limited access to technology and low levels of literacy and legal knowledge can increase barriers to accessing digital services and thwart the stated aims. Therefore accessibility for all must be ensured, in terms of support measures and technology.

Brussels, 19 May 2022

Christa Schweng
The president of the European Economic and Social Committee