EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE Statement on the European Declaration on Digital Rights and principles

16/02/2023

EXECUTIVE SUMMARY

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 46 countries, and through them more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

On 15 December 2022, the European Parliament, the EU Council and the European Commission signed the Declaration on Digital Rights and Principles. The Declaration promotes a European way for the digital transition, which is based on European values and benefits all individuals and businesses. It outlines **six digital rights and principles**: (1) putting people at the centre of the digital transformation; (2) solidarity and inclusion; (3) freedom of choice; (4) participation in the digital public space; (5) safety, security and empowerment; and (6) sustainability.

1. General comments

The CCBE welcomes the declaration and commitments of the EU institutions and recognises its general purpose of safeguarding and enforcing European values and fundamental rights in the digital transformation of our societies. It notes that the text is only of a declaratory nature, as indicated in its preamble, and does not affect the content of legal rules or their application.

Within this statement, the CCBE would like to underline the specific issues raised by the digitalisation of Justice. While it may foster the interoperability of national systems, and supports the uptake of new technologies in the day-to-day functioning of our justice systems, digitalisation needs to be coupled with sufficient safeguards and due process procedures in order to uphold fair trial rights, including the protection of professional secrecy and legal professional privilege. In this regard, the CCBE estimates that endeavours on e-justice must respect and ensure fundamental rights and principles, as they are recognised by the **EU Charter of Fundamental Rights and the European Convention on Human rights**. The CCBE stresses that e-justice systems need to be secure and support an "**electronic equality of arms**" and **''access to justice''**. In other words, digital procedures should facilitate all parties in a trial and not only one party to the possible disadvantage of the other party. Also, they should ensure that all parties enjoy at least the full procedural rights that they previously had under paper-based systems.

2. Comments on the content of the declaration

2.1. Solidarity and inclusion

Regarding the **second principle on s*olidary and inclusion***, the CCBE notes the existence of a "digital gap" which it considers to be significant within and between Member States. Insofar as digital technology should be used to simplify access to justice, it should not have the opposite effect. **Therefore, digitalisation should not be full or completely mandatory, should be accompanied by sufficient training for citizens, professionals and administrations, and should always be human centred**. In this regard, the CCBE would like to highlight the recent judgement of the European Court of Human Rights, in the case ***Xavier Lucas v. France***, from 9 June 2022[1].

2.2. Freedom of choice

With regard to the **third principle on the *freedom of choice*** indicating that everyone should be empowered to benefit from the advantages of AI by making their own informed choices in the digital environment while being protected against risks and harm; the CCBE reiterates its specific comments on the use of AI in our justice systems laid down in its **position paper on the AI Act**[2] and in its former contributions[3]. In particular, the CCBE considers that the "*entire decision-making process must remain a human-driven activity and human judges must be required to take full responsibility for all decisions. A right to a human judge should be guaranteed at all stages of the proceedings*". The principles of transparency and explainability must be strictly observed. The use of AI tools which may infringe a person's fundamental rights should be excluded, for example for the purposes of so-called 'predictive policing' and for the purposes of determining risks of future offending as an aid to the making of decisions as to the granting of bail, the imposing of a sentence, following conviction, the making of decisions concerning probation and, generally, during prosecution and trial.

[1] ECHR, 9 June 2022, Xavier Lucas v. France, application 15567/20, §57-59. The Court held that "*by giving precedence to the rule that proceedings in the Court of Appeal were to be issued electronically, while disregarding the practical hurdles faced by the applicant in doing so, the Court of Cassation had taken a formalistic approach that was not needed to ensure legal certainty or the proper administration of justice and which therefore had to be regarded as excessive*". The Court concludes that "*a disproportionate burden had been placed on the applicant, upsetting the proper balance between, on the one hand, the legitimate concern of ensuring adherence to the formalities for the issuance of court proceedings and, on the other, the right of access to a court*"; therefore there has been a violation of Article 6§1 of the Convention.

[2] CCBE position paper on the Artificial Intelligence Act (08/10/2021)

[3] CCBE Response to the consultation on the European Commission's White Paper on Artificial Intelligence (05/06/2020): https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20200605_CCBE-Response-to-the-consultation-regarding-the-European-Commission-s-White-Paper-on-AI.pdf ; CCBE considerations on the Legal Aspects of AI (20/02/2020): https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf

2.3. Safety, security and empowerment

The CCBE welcomes the principle 5 on "safety, security and empowerment", which states that everyone should have access to safe and privacy-protected products and services and have control over their personal data online, and that everyone has the right to the confidentiality of their communications and the information on their electronic devices, and no one shall be subjected to unlawful online surveillance or interception measures. **The CCBE invites European authorities to take consideration of its recommendations on the protection of fundamental rights in the context of 'national security[4] as well as on the protection of client confidentiality within the context of surveillance activities[5]. It considers that any form of surveillance should be kept at a minimum and subject to a clear regulatory framework.**

Such framework should ban mass surveillance and ensure that the principle of confidentiality of the communications between lawyers and their clients and professional secrecy are out of the scope of surveillance activities[6]. In this regard, the technology used by private actors, like internet service providers, and public actors, like law enforcement authorities, to collect, process and exchange personal data and to conduct surveillance activities should ensure that there is no interference with any kind of data protected by professional secrecy. Professional secrecy by design and by default should be the rule. Furthermore, the CCBE considers that any surveillance activity should be regulated with adequate specificity and transparency.

[4] CCBE recommendations on the protection of fundamental rights in the context of 'national security, 2019

[5] CCBE recommendations on the protection of client confidentiality within the context of surveillance activities, 2016

[6] See the Resolution of the European Parliament, 'Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens', 29 October 2015, §43