



OPINION

European Economic and Social Committee

Digital identity, data sovereignty and the path to a just digital transition for citizens living in the information society

Digital identity, data sovereignty and the path to a just digital transition for citizens living in
the information society
(own-initiative opinion)

TEN/773

Rapporteur: **Dumitru FORNEA**

www.eesc.europa.eu

EN

Legal basis	Rule 52(2) of the Rules of Procedure Own-initiative opinion
Plenary Assembly decision	20/01/2022
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	21/06/2022
Adopted at plenary	14/07/2022
Plenary session No	571
Outcome of vote (for/against/abstentions)	179/1/3

1. **Conclusions and recommendations**

- 1.1 Technological progress and the evolution of digital technologies, biotechnologies and electronic communications systems have created important opportunities to consolidate economically prosperous, more inclusive and just societies. At the same time, a number of dangerous threats to humanity have developed.
- 1.2 In order to maintain the security of humankind and the social fabric necessary for every individual to live a fulfilling life on this planet, we must ensure that the new tools of governance that are imposed with the digital and industrial revolution are not oppressive and do not make the daily lives of individuals conditional on compulsory incorporation in digital technological systems controlled in an undemocratic way.
- 1.3 Public institutions are vulnerable to non-state actors with direct access to knowledge, patents, technologies and investment funds. The EESC believes that European technological sovereignty must be included in all future policy developments and the legislation must be supplemented with explicit and fully applicable regulations and common standards across all Member States.
- 1.4 Technological developments affect many citizens' rights and freedoms. The Committee requires that all sectors that use personal data and biodata should be regulated in a clear manner and in full compliance with fundamental human rights, and calls for the GDPR to be updated accordingly.
- 1.5 The EESC is convinced that digital identity, digital means of payment and incorporation into virtual and augmented reality platforms should remain tools that only complement the physical existence that we knew before the adoption of these technologies and should not completely and abusively replace other existential patterns that have been developed and perfected by humans over thousands of years of existence.
- 1.6 The EESC calls for clear anti-discrimination provisions in all future legislative proposals on digital identity and is totally against the introduction of a system that keeps close tabs on European citizens, tracks them and/or monitors their activities and behaviour. Furthermore, the Committee deems it necessary that organised civil society be thoroughly involved in the implementation process.
- 1.7 The EESC has come to the conclusion that any initiative to integrate citizens into the European digital identity system should be based on impact studies and comprehensive sociological surveys. The final decision should only be made with the citizen's informed and freely expressed consent.
- 1.8 The EESC believes that in order to move democratically towards a fair digital society that is accepted by EU citizens, the European Commission must carry out impact assessments on:
 - The enormous and 24/7 need for energy to maintain the global technological infrastructure to support uninterrupted and secure access to a digital system aimed at transferring the critical and strategic functionalities of human society;

- The impact of digitisation and automation of human interaction on quality of life and working conditions, especially in terms of human relations, increasing the prevalence of loneliness, mental health issues, declining cognitive and emotional intelligence and increased risk of social alienation;
 - The political, economic and social measures needed to adapt society to the dramatic quantitative changes in the labour market;
 - Cyber security, in the context of which the diversity and complexity of hackers' activities has increased and regarding the conditions of the accelerated development of the Internet of Things which make access protocols vulnerable and permeable.
- 1.9 The EESC concludes that data security should be non-negotiable and is disappointed that the security of the future digital European wallet is not the top priority in the Commission's legislative proposal.
- 1.10 The EESC considers that full accountability for possible malfunctions must be clearly provided for in all the EU legislative proposals on artificial intelligence. The right balance must be struck between not disclosing commercial secrets and ensuring transparent and traceable developments.
- 1.11 The Committee was the first European institution to call for a "human in command" approach and reiterates the need for several layers of control to ensure that.
- 1.12 The EESC is totally against private facial recognition databases except for crime purposes and any type of social scoring system, as these violate EU fundamental values and rights.
- 1.13 The Committee believes that the data produced in the EU should be stored on EU soil and should be protected from any extra-territorial access. Furthermore, the EESC believes that informed consent on data use must be implemented for both personal and non-personal data and calls once again for the GDPR to be upgraded in this regard.
- 1.14 The EESC is worried about the growing disparities between Member States and the lack of protection of vulnerable groups and calls again for an EU that embraces digital inclusion where no one is left behind. Special attention should be paid to the older generation.
- 1.15 The Committee calls for a strong European digital education system that can prepare the workforce for technological challenges and help them acquire high quality jobs. Digital literacy programmes must be implemented in all Member States, together with lifelong digital learning programmes, vocabulary tutorials and practical training.
- 1.16 The Committee considers engaging employees in the digital transition to be vital so they can understand the future risks and opportunities so that knowledge can be transferred and new skills can be acquired.

2. Background

- 2.1 European citizens are interested in developments in implementing digital technology solutions to simplify the administrative procedures necessary for dealing with authorities or in everyday life in society. This opinion aims to raise awareness among national and European decision-makers about the concerns of organised civil society related to the potential adverse societal effects associated with the accelerated deployment of digital technologies.
- 2.2 The COVID-19 pandemic has speeded up the digital transformation of societies and forced citizens to embrace new technologies for work, study and other daily activities. It has provided opportunities for businesses and citizens to upgrade digitally and progress.
- 2.3 The benefits of the widespread implementation of a digital identity are widely explained in various documents of the European institutions and global international organisations. In this respect, the most recent document is the Proposal for a Regulation as regards establishing a framework for European Digital Identity¹, published on 3 June 2021.
- 2.4 The European Commission aims to provide a European digital identity framework based on the revision of the current framework, so that at least 80% of citizens have an electronic identification solution to access essential public services by 2030². Public authorities must be equipped with the necessary human and financial resources to be able to include and control digital technological developments.
- 2.5 As evidence of this, it should be noted that the Digital Economy and Society Index (DESI)³ published by the European Commission in 2021 shows that, in 2020, the percentage of people with at least basic digital skills was 56%. However, a large part of the EU population does not yet have basic digital skills, even though most jobs require them. Many citizens claim to have digital skills, but on closer inspection, these are no more than the ability to make basic use of the opportunities offered by the internet (browsing and social networking) and the software packages offered by Microsoft Office or Mac OS.
- 2.6 Regarding artificial intelligence, a recent study released by the European Investment Bank⁴ shows that Europe is still lagging behind other economic world powers. It mentions that the US and China together account for more than 80% of the EUR 25 billion in annual equity investments in AI and blockchain technologies. The EU only accounts for 7%, and the total investment gap is between EUR 5 and 10 billion per year.

1 [Proposal for a regulation of the European parliament and of the Council amending Regulation \(EU\) No 910/2014 as regards establishing a framework for a European Digital Identity](#), COM/2021/281 final.

2 [Digital Identity for all Europeans](#)

3 <https://digital-strategy.ec.europa.eu/en/policies/desi>.

4 [EIB study: Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy](#).

2.7 The Commission has proposed to close this gap and provide EUR 1 billion investment per year in AI, which should be supplemented by private investment and Member States' own resources. The target is to reach EUR 20 billion in investment per year over the coming decade⁵.

3. **General Comments**

3.1 Technological progress in general and the evolution of digital technologies, biotechnologies and electronic communications systems over the last two decades have created enormous opportunities globally to consolidate economically prosperous, more inclusive and just societies.

3.2 At the same time, without a new social contract and a regulatory framework adapted to these new technologies with disruptive impact, a number of dangerous threats to humanity have developed (like job loss due to automation advancements and deployment, privacy violations, algorithmic bias caused by bad data, market volatility, etc.), especially given the constant attempts of global tech giants to impose their products and services, by-passing the existing body of legislation at international and national level that guarantees fundamental human rights.

3.3 International and national government institutions are vulnerable to non-state actors with direct access to knowledge, patents, technologies and investment funds, as often the staff of these institutions fail to grasp the full societal impact of new technologies on the rights of citizens and consumers. The Committee is convinced that EU technological sovereignty considerations must be included in all future policy developments.

3.4 The EESC calls for the legislation to be clarified and supplemented with explicit and fully applicable regulations and common standards across all Member States, including related responsibilities, regarding the fact that digital identity-related technologies are largely managed by computer algorithms and artificial intelligence, which cannot be held responsible for the mistakes they make.

3.5 There are already many documented situations, which have been studied in detail, in which people are affected and unjustly condemned for the wrong decisions of computer algorithms and artificial intelligence. For example, decision-makers in the security and police forces are misled by the incorrect results of computer algorithms such as "artificial intelligence", "facial recognition", "machine learning", "data analysis and forecasting", "timesheets and scores", etc. As a result, many citizens' rights and freedoms are affected.

3.6 Therefore, the legal rules that will be developed to cover the field of digital identity and its related technologies must be based primarily on full transparency, correct and complete information of users and free informed consent, and must ensure full protection that caters for all the cyber vulnerabilities of mobile communication networks and their devices, etc. For these reasons, the EESC requires that all sectors that use personal data and biodata, such as digital identity or the 5G mobile communications networks, artificial intelligence and so forth must be regulated in a distinct, clear manner and in full compliance with fundamental human rights.

⁵ [European Commission - A European approach to artificial intelligence.](#)

4. **Specific comments**

Digital identity

- 4.1 When it comes to digital ID implementation in Europe, data management is vital to ensure citizen's protection and safeguard their privacy. Full compliance with General Data Protection Regulation (GDPR) must be ensured.
- 4.2 European citizens are at the centre of any programmes and policies implemented in the EU. The EESC appreciates and supports the release of the Commission Proposal on Digital Identity for all Europeans⁶, which specifies that the choice of whether or not to use a digital ID must lie with the individual. Still, the Committee considers that the impact of the exclusion of certain citizens who will not opt for a digital ID has been downplayed and insists that the right to be forgotten and right to disconnect be clearly implemented in the EU legislation.
- 4.3 The EESC calls for clear anti-discrimination provisions in all future legislative proposals on the subject. Whatever the reason why any citizen might decide not to use such a feature, be it for data protection or anonymity reasons or other, they must not be placed at a disadvantage compared to active users or marginalised. Individual data should always remain the property of the respective individual while protection of human rights must underpin the implementation of digital ID. In order to guarantee data protection and security, as well as respect for private life, the Committee proposes that the digital identity of EU citizens be managed, in each Member State, by a public service body, under the authority of the State and subject to democratic control by national parliaments.
- 4.4 The introduction of a digital ID in Europe should have the purpose of enabling secure and easy connectivity for consumers. It must provide, among other things, improved data and public service delivery, enhanced targeted government programmes and greater credit market efficiency. The EESC is in favour of such a scenario. However, the Committee notes that the implementation of the digital ID entails a series of risks in terms of privacy and data protection and is totally against the introduction of a system that keeps close tabs on European citizens, tracks them and/or monitors their activities and behaviour.
- 4.5 Cybersecurity is an important aspect of the implementation, with the risk of hacking important personal and financial data being high. The EESC is looking forward to the final version of the proposed legislation and the agreement between Member States on the standards, technical specifications and interoperability aspects, which should be in place by October 2022. The EESC considers that organised civil society, including social partners, NGOs and academia, must be thoroughly involved in the implementation process.
- 4.6 Fraud remains one of the greatest risks connected to the implementation of the digital ID. Phishing messages that we all receive today will be multiplied and targeted at the most vulnerable groups in Europe. The EESC considers that the security issues around this matter

⁶ [Digital Identity for all Europeans, COM/2021/281 final](#).

have not been thoroughly quantified and is disappointed that the security of the future digital wallet is not the most important issue in the EC proposal establishing a framework for a European Digital Identity. Synthetic ID fraud has happened in other parts of the world where similar systems are implemented and the EU should familiarise itself with and tackle these issues before implementation. Therefore, the Committee considers that data security should be non-negotiable.

AI – Artificial intelligence

- 4.7 The digital single market needs AI to evolve and progress. Artificial intelligence is based on algorithms that require huge amounts of private data and metadata. Society needs to benefit from technological developments and algorithm-based applied science. However, when implementing AI technologies it must be ensured that the historically marginalised communities are able to cope with the programmes and that the existing social disparities are not exacerbated.
- 4.8 The EESC was the first European institution to call for a human in command approach when dealing with AI systems⁷. The EESC reaffirms that it is paramount that humans have the last say and are in full control of decision-making processes when it comes to machine developments.
- 4.9 Intellectual property protection can be used as an argument for non-transparent AI developments. The EESC considers that the right balance must be struck between not disclosing commercial secrets and ensuring transparent and traceable developments. Furthermore, accountability for possible malfunctions must be clearly provided for in all the EU legislative proposals on artificial intelligence and liability should be placed on the developers, coders, AI designers and rightful owners.
- 4.10 The Committee feels that AI technologies must be implemented in a socially sustainable way, taking into consideration human rights, European values, gender equality, cultural diversity, the interests of disadvantaged groups and intellectual property rights.
- 4.11 Further progress is needed on the GDPR regulation in order to make sure that algorithms are in full compliance with and respect European law and the Committee requests the development of common ethical rules that ensure free access to the source codes of algorithms.
- 4.12 AI has the potential to contribute to reaching the climate and environmental goals, but one must take into consideration the huge amount of energy that is used for running these digital systems, as well as other challenges related to internalising the external costs. The EESC proposes enhanced monitoring of this aspect and calls for the digital companies to make progress on carbon emission reduction.
- 4.13 In key areas like defence or cybersecurity, control of humans over robots must be guaranteed and the EESC calls for a very specific framework at EU level that ensures this, and that human

⁷ [OJ C 288, 31.8.2017, p. 1.](#)

intervention must always be possible to repair the errors of any automated decision-making system.

- 4.14 The EESC is wholly against private facial recognition databases, except for crime purposes, and any type of social scoring system, as these violate EU fundamental values and rights.
- 4.15 With regard to the social aspects, the EESC is worried that AI developments will have a huge impact on the labour markets, potentially causing an unemployment crisis. Furthermore, they could impact on human behaviour and lead to laziness and superficiality.

Big data

- 4.16 The EESC welcomes the Data Act⁸ issued by the European Commission in February 2022 and considers it an ethical framework for the transparent processing of personal data, with the citizens and businesses that generate them in full control. It also makes it possible for data to be used by a larger number of stakeholders and citizens, with extended benefits for consumers, businesses and public authorities, leading therefore to a fair data-driven economy.
- 4.17 Large amounts of data are now available to public authorities and a handful of big tech giants such as Google, Facebook (Meta), TikTok or Amazon. Unfortunately, only a limited number of stakeholders benefit today from it and the EESC is worried that the data produced in the EU is stored, processed and produces value outside Europe⁹. The Committee considers that EU digital sovereignty will be hard to achieve without its own EU digital tech giants, without storing European data on EU soil and without protection of these data from any extra-territorial access.
- 4.18 Big data management must always respect human rights as enshrined in Article 21 of the Charter of Fundamental Rights of the European Union¹⁰, especially when algorithms are used in the decision-making process. EU-based cloud providers hold only a small part of the international market, which is largely dominated by US companies. This puts the EU at disadvantage and is limiting investment possibilities in the data processing market. It is also hindering the competitiveness of large companies and their possibility to grow and gain markets, and prevents SMEs from scaling up. The Committee salutes the EC Communication on *A competition policy fit for new challenges*¹¹ and the importance placed on digital transformation when reshaping the future EU competition framework.
- 4.19 The Committee considers that informed consent on data use must be implemented for both personal and non-personal data. The EESC calls once again for the GDPR to be upgraded in this regard.

⁸ [European Commission – Data Act.](#)

⁹ Eurostat reports that only 36% of EU enterprises used cloud services in 2020 and most of them for email and storage, with only 19% of cloud companies used.

¹⁰ [OJ C 326, 26.10.2012, p. 391.](#)

¹¹ [EC Communication – A competition policy fit for new challenges](#) (COM/2021/713 final)

Just digital transition and digital literacy in the EU

- 4.20 The Committee notes a changing labour market with more and more sectors of the economy complaining of the lack of a skilled and qualified labour force. It also notes a decline in qualifications and lack of specific know-how and expertise.
- 4.21 The EESC has called in previous opinions for a Union that embraces digital inclusion where no one is left behind. Years later, disparities between Member States are growing and vulnerable groups are still unprotected, especially the older population, which is the most exposed.
- 4.22 The Committee is worried about the existing digital divide in the EU and calls for digital literacy programmes to be implemented in all Member States in a coordinated manner and calls for lifelong digital learning, including open-source solutions as free alternatives to commercial ones, to become a reality in the EU. Creating digital skills begins with vocabulary tutorials and finishes with practical training.
- 4.23 Engaging employees in the digital transition is vital so they can understand the future risks and opportunities at the same time. Changing workplace environments require knowledge to be transferred and new skills to be acquired, but also improved working conditions for people working through digital labour platforms.
- 4.24 The EESC calls for a strong European digital education system that can prepare the workforce for technological challenges and help them acquire high quality jobs, and recalls in this regard the European Social Partners Framework Agreement on Digitalisation.
- 4.25 The Committee has already called for the need for STEM solid competences in science, technology, engineering and mathematics to be further improved¹².

Brussels, 14 July 2022

Christa SCHWENG
The president of the European Economic and Social Committee

¹² [OJ C 14, 15.1.2020, p. 46](#), [OJ C 10, 11.1.2021, p. 40](#), [OJ C 228, 5.7.2019, p. 16](#), [OJ C 75, 10.3.2017, p. 6](#), [OJ C 374 16.9.2021, p. 11](#).