



*European Economic and Social Committee*

**TEN/679**

**The digital revolution in view of citizens' needs and rights**

## **OPINION**

European Economic and Social Committee

**The digital revolution in view of citizens' needs and rights**

[Own-initiative opinion]

Rapporteur: **Ulrich SAMM**

Plenary Assembly decision	12/7/2018
Legal basis	Rule 29(2) of the Rules of Procedure Own-initiative opinion
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	11/02/2019
Adopted at plenary	20/02/2019
Plenary session No	541
Outcome of vote (for/against/abstentions)	129/2/1

## 1. Conclusions and recommendations

- 1.1 The current **digital revolution** has the potential to fundamentally change society, the economy and the workplace and provide long-term benefits for both economic growth and quality of life with an impact on all sectors, changing the way we live, work and communicate. The EESC has clearly expressed its view that the transformation – made by humans – should benefit everyone. The EESC therefore welcomes all political and civil society actions that help European citizens. This opinion primarily addresses citizens' needs and concerns, be it as employees, employers or as consumers in general, and identifies areas where the involvement of civil society is key. Only by proactively shaping the digital transition will we make it a success story.
- 1.2 The progress of digitalisation, in particular when new digital products and services are introduced, can be very fast (as in the case of mobile/smartphones) or it can be slow in certain areas, where the public and society in general do not accept the technology without question, as is the case when human **autonomy, responsibility, security, dignity** and **privacy** are affected.
- 1.3 Digitalisation offers a wealth of new possibilities allowing people to make choices for a better life in an unprecedented way. On the other hand, the more digitalisation dominates our life, the more we can also be manipulated. This can undermine our **autonomy** in areas such as driving cars, choosing food, taking care of our health, heating our homes, smoking, drinking, managing our finances and many more. The EESC calls for transparent rules to be developed, adapted and applied to these rapidly evolving technologies. Good persuasive technology should involve training, not manipulation, and comply with the principle of people's free choice, to guarantee human autonomy.
- 1.4 The EESC has a clear view on the question of the extent to which it is ethically acceptable to delegate making choices (with moral implications) to systems based on AI: automated systems, regardless of how complex they are, have to operate according to the human-in-command principle. Only humans make the final decision and take **responsibility** for it.
- 1.5 With more home automation, a range of entry points for hackers is evolving. There is a need to inform consumers about these risks and provide support for **security** measures, in particular when hackers try to take over control of smart devices. The EESC calls on the EU to revisit existing security regulations and to develop and adapt strict security rules for new evolving technologies for the protection of citizens in their homes.
- 1.6 The EESC welcomes the approach of improving **road safety** by introducing more digital technology in cars, but also expresses worries about the slow pace of these improvements. To accelerate the transition to more automatic driving, the EESC calls for the development of EU-incentives to address the demanding costs (need to buy new cars) and the insufficient acceptance of assistance systems (complexity, lack of training). The EESC believes that a European strategy must be developed to adapt and modify our road system so that fully autonomous vehicles with 100% safety can become a success.
- 1.7 The EESC calls for the GDPR to be adapted and overhauled in view of the fast-changing digital technology. New facial recognition technologies, in particular, are a threat to our **privacy**. As

this technology becomes cheaper and easily accessible to all, it could ultimately lead to a situation where it is no longer possible to walk down the street or go shopping anonymously. The threat to privacy and autonomy is even greater when these technologies are used for profiling or scoring. The EESC insists that people should have the right to be private in public spaces too. The EESC urges the Commission to regularly revise the GDPR and related regulations depending on how fast these technologies change.

- 1.8 The individual **consumer**, who does not have professional digital skills, needs strong support in using complex digital systems, be they home appliances or digital platforms. User manuals can be very long and permission to use certain data is often given unwittingly. The EESC is convinced that transparency is not sufficient: simplification and standardised procedures across the EU are therefore needed to help the consumer.
- 1.9 Digital platforms can easily track their users with simple tools. This means that for the protection of privacy, the GDPR is insufficient when data is purposely misused without people's knowledge. The EESC is convinced that privacy can only be guaranteed by additionally **restricting access** to sensitive data to only a limited number of certified people. Security measures must be developed to the highest, most trustworthy standards, including regular verification by independent EU bodies.
- 1.10 The EESC is worried that surveillance systems based on **biometrics** can result in misclassification and stigmatisation, by automatically putting someone in a certain category, such as that of terrorist, criminal or unreliable individual. Systems that automatically identify and classify people as suspicious should never work without close human interaction and thorough verification.
- 1.11 The use of robotics in the healthcare sector is anticipated. But robots are devices that are unable to replicate the empathic capacities and reciprocity of human care relationships. If not used under certain framework conditions, robots can undermine **human dignity**. Care robots, therefore, should only be used for care tasks requiring no emotional, intimate or personal involvement.
- 1.12 The EESC recommends, whenever new automation systems are planned in industry, commerce and service sector, using objective scientific methods to optimise and evaluate human-machine interaction. The scientific methods of **cognitive ergonomics** make it possible to objectively assess mental demands while dealing with new technical assistance systems. It combines different research disciplines, such as psychology and ergonomics, to evaluate user interfaces. The EESC is convinced that only with human centred design will digitalisation be successful in the long term.
- 1.13 The EESC calls for assessing the differences in **regional developments** and the scale of possible social inequalities and its possible effects on the EU's integrity caused by an uneven access to new digital technologies and a skills gap.

## 2. Introduction

- 2.1 The EESC welcomed in previous opinions<sup>1</sup> the fact that the European Commission has established a **Digital Europe** programme, which underscores the intention to make Europe a leading player in digitalisation and to increase its economic strength and competitiveness on the world stage, enabling a digital single market to come into being and shaping the digital transformation in a positive way for all citizens of Europe.
- 2.2 The current **digital revolution** has changed society and will do so even more in the future. These changes affect the economy and the workplace, providing long-term benefits for both economic growth and quality of life with an impact on all sectors, changing the way we live, work and communicate. The EESC has clearly expressed its view<sup>2</sup> that the transformation – made by humans – should benefit everyone. The EESC therefore welcomes all political and civil society actions that help European citizens. This opinion focuses primarily on the needs and concerns of **citizens**, whether as employees, employers or as consumers in general. It identifies areas where civil society involvement is key to proactively shaping the digital transition and making it a success story.
- 2.3 The progress of digitalisation, in particular when new digital products and services are introduced, can be very fast (as in the case of mobile/smartphones) or it can be slow in certain areas, where the public and society in general do not accept the technology without question, as it is the case when human **autonomy, responsibility, security, dignity** and **privacy** are affected. The analysis in this opinion is partly based on a publication by Royakkers et al., Ethics Inf Technol (2018).
- 2.4 The development of new digital applications is being promoted by many enthusiasts in industry, laboratories and universities, not only, as many people believe, by internet giants such as Google, Apple, Facebook, Amazon or Microsoft. This enthusiasm is shared by many in society; however, there is also a significant minority of people who are sceptical or anxious, either because of threats to their privacy, autonomy, security etc., or perhaps owing to a lack of knowledge and a basic fear of the future. The digital transition is not driven only by technology. People's and society's needs and desires, as well as their rights, should have a decisive impact on further technological development. For a successful digital transition, involving people in design and decision-making processes is a clear challenge for all, and for civil society in particular. This also means that access to secure and affordable internet connections should be guaranteed so that we avoid discrimination and exclusion.

## 3. The speed of the digital transition

- 3.1 The digital revolution is the shift from mechanical and analogue electronic technology to digital electronics, which took place somewhere between the late 1950s and the late 1970s, with the adoption and proliferation of digital mainframe computers and personal computers. During the

---

<sup>1</sup> [OJ C 62, 15.2.2019, p. 292.](#)

<sup>2</sup> [OJ C 434, 15.12.2017, p. 30; OJ C 434, 15.12.2017, p. 36; OJ C 237, 6.7.2018, p. 8; OJ C 367, 10.10.2018, p. 15.](#)

1980s, digital technology became widespread in many areas. Tablet and smartphone use is now on the way to outstripping personal computer use.

- 3.2 Starting in 1991, the accessibility of the **worldwide web** for the public provided a new infrastructure that made it possible to connect digital devices, creating new functions going far beyond the features of a single digital device alone. The combination of these technologies has fundamentally transformed the way we communicate, the way we work and the way we do business. **Digital platforms** have given rise to radically new ways of doing things – Airbnb, Uber and Amazon, to name just a few examples, have in the space of a few years become major economic players.
- 3.3 It seems there are no limits to further digitalisation. The increasing use of **smart sensors** makes it possible to read and process data (location, movement, environmental data, biological data, chemical data) relating to any kind of object (**Internet of Things**). There is virtually no limit to the number of sensors, so it is theoretically possible to generate a digital map of our whole physical environment. In the future, fast broadband (5G) will make it possible to react to sensor data in real time.
- 3.4 Huge amounts of data from sensors and platform activities (**big data**) will be processed by computer programmes based on certain algorithms. Programmers will be able to either narrowly define these algorithms, or generate them dynamically using a set of input data (**machine learning** or **AI**). From AI, in particular, many are expecting significant technological breakthroughs<sup>3</sup>. The question how far we allow machines to make choices (with moral implications) is of crucial importance and requires social and political control. There is already a strong demand for limitations to be placed on automatic computer systems in certain areas (such as fintech) because of a significant loss of control and lack of transparency.
- 3.5 The pace of the development of digitalisation in society is very fast. Public organisations and businesses are adopting plenty of new approaches, as attested by pilot projects or products already entering the market. The **market penetration** of these new products can be very, very different depending on the sector. Conversely, it can be slow in certain areas, where the technology is not accepted without question, as described in the following paragraphs.
- 3.6 A typical example of the Internet of Things with limited acceptance is home automation or **smart home** systems, to control lighting, heating, entertainment devices or units, household appliances and much more. Access control and alarm systems with security cameras can upload videos. Home automation systems lack technical standards, making it hard to develop applications that work consistently for different objects. They may also require advanced skills and continuous updating. Another difficulty lies in the fact that most homes are shared environments, with people who have different interests, skills and abilities (children, older people and guests, for example). It is much easier to live in a smart home that manages the life of one person.

---

<sup>3</sup> [OJ C 288, 31.8.2017, p. 1.](#)

- 3.7 Smart car sensors make **connected and automated mobility** possible, by offering a wealth of new features for better convenience and safety and eventually, with full automation, the highest degree of safety in road transport<sup>4</sup>. The technology for automatic driving is fairly mature, but for a number of reasons its widespread application is only developing slowly. Firstly, a high degree of assisted driving is possible only in new cars, where the sensors and central computing units are an integral part of the vehicle. The costs of this for individuals and society are an obstacle to market penetration. Secondly, a growing number of assistance systems can make driving a car much more complex, causing limited acceptance. Thirdly, the demand that fully autonomous vehicles be 100% safe is a big obstacle as long as these vehicles share the road with conventional cars and other road users. Fully automatic vehicles are a challenge because they make it necessary to significantly redesign the road system.
- 3.8 Google and Facebook already use **AI** intensively and successfully to "optimise" information display and advertising. But there are many more areas where AI can and will be used, providing powerful assistance in cognitive work, as in knowledge-based professions. Some of these areas, however, may develop more slowly than expected due to a fundamental problem, as stated recently: "a limitation for AI is not the technology (computer power) but our lack of fundamental understanding how humans exactly learn and think". Thinking outside the box and using life experience is still a human privilege.
- 3.9 There are some very successful pioneers who have converted public services into flexible e-solutions. For example, in Estonia a multitude of services such as **e-government**, e-tax, e-health or e-voting are well accepted, widely used and seen by many as a role model for technology that should be implemented in all EU countries, preferably with the same standards, to enable interoperability. Only with an EU-wide strategy and well funded projects can we overcome the obstacles posed by the existing large diversity of regions, institutions and cultures, and the demand for subsidiarity over central government.

#### 4. **Concerns and recommendations**

- 4.1 In 2017, the European Commission published a Eurobarometer survey<sup>5</sup> showing that 76% of people who use the internet every day say the impact of these technologies on their quality of life has been positive, but 38% of people never use the internet. The latter percentage may be due to a lack of digital skills, but there are also a significant number of people who might have the skills but have serious concerns about internet use, making them hesitate to follow suit. This point of view has to be respected and taken seriously. Concern is expressed in particular over the issues of autonomy, responsibility, security, human dignity, privacy and working conditions, as explained below.

---

<sup>4</sup> [OJ C 62, 15.2.2019, p.274.](#)

<sup>5</sup> [Special Eurobarometer 460 – Survey conducted by TNS Opinion & Social, March 2017.](#)

## 4.2 **Autonomy**

- 4.2.1 We speak of **paternalism** if someone professes to know better what is good for other people than they do themselves. With technological paternalism, the paternalism is "delegated" to technology. Paternalism can be persuasive or compelling. Good persuasive technology should involve training, not manipulation, and comply with the requirement of people's free choice, to guarantee human autonomy. Digitalisation offers a wealth of new possibilities allowing people to make choices for a better life in an unprecedented way. On the other hand, the more digitalisation dominates our life, the more we can be manipulated. This undermines our autonomy in areas such as car driving, choosing food, taking care of our health, heating our homes, smoking, drinking, managing our finances and, as seen in recent events, even elections which, if manipulated, can pose a threat to democracy. The EESC calls for the development, adaptation and application of transparent rules and when, appropriate, strict legal measures for these rapidly evolving technologies.
- 4.2.2 The most striking example of extreme use of digital technology to influence people can be found in **China**. For each of its citizens the Chinese Government keeps a citizen score, to help determine if someone is eligible for a loan, a visa or a job. This is in sharp contrast to European values and rights (data protection, privacy, social protection, sustainability).
- 4.2.3 A trend has been observed where people develop a growing desire for a more **analogue life**, at least for a certain part of their time. There are sleep-away camps, where adults go to unplug for an off-the-grid weekend, or people spend time offline to focus on children, families and friends – meaning no phone in hand. There is a stable demand for things now considered analogue, although a digital alternative exists: books, music created without computers, vinyl records, paper, pens and much more. A number of high-level executives have been known to bankrupt their email traffic once in a while. This means deleting every email in their inbox or closing their account altogether, to recover from the deluge of electronic communication. The EESC believes that the digital transition also needs such counterweights to succeed and be acceptable to all, and warns against pushing too much to replace analogue techniques.

## 4.3 **Responsibility**

"Man-out-of-the-loop" refers to **full automation**, where the system makes a decision without human intervention. Examples include knowledge systems that make medical diagnoses based on a large amount of information, or military robots that make life or death decisions using information from various sources. The crucial, frequently asked question is: to what extent is it ethically acceptable to delegate making choices (with moral implications) to systems based on AI? The EESC has already expressed a clear view on this<sup>6</sup>: the terms "responsibility" and "moral" are exclusively linked to human beings, while certain mental or personality traits cannot be attributed to robots. Automated systems, regardless of how complex they are, have to operate according to the **human-in-command** principle. Only humans make the final decision and take responsibility for it.

---

<sup>6</sup> [OJ C 288, 31.8.2017, p. 1.](#)

#### 4.4 Security and consumers

4.4.1 As hot new gadgets make our homes smarter, they are also making them more vulnerable. With more of our devices connecting to the internet – smart TVs, webcams, gaming consoles, smartwatches – it is crucial to have a good defence plan for your home network. Smartwatches and other wearable devices are an extension of a smartphone, giving instant access to powerful apps, emails, text messages and the web. Besides extracting information that is valuable to hackers, they can also **take over control** of smart devices. Security researchers have demonstrated how simple it is to hack the toy doll Cayla or that one could hack even an insulin pump or spy on a smartwatch wearer. Consumers have to be made aware of these risks. The EESC calls on the EU to revisit existing security regulations and to develop and adapt strict security rules for new evolving technologies for the protection of citizens in their homes.

4.4.2 The application of **biometrics** (face recognition, fingerprints, iris scan) is great if the system works well. But for people whom the system incorrectly identifies as suspicious, it is often very difficult to rectify errors. The application of biometrics can result in **misclassification** and **stigmatisation**, by automatically putting someone in a certain category, such as that of terrorist, criminal or unreliable individual. This can lead to a reversal of the presumption of innocence. It also appears that biometrics cannot be used for everyone. For example, 2% of people's fingerprints cannot be "read" because they are senior citizens or because of certain professions or chemotherapy treatments. The digital systems our society uses must be designed not to exclude or discriminate against people who do not meet certain standard criteria. Systems that automatically classify people as suspicious should never work without close human interaction and thorough verification.

4.4.3 **Identity fraud** is a major problem. Identity fraud is the intentional obtaining, appropriating, owning or creating of false identifiers, committing or intending to commit unlawful conduct. Our society needs sufficient legal support to protect the victims of such identity fraud.

#### 4.5 Human dignity

4.5.1 The use of robotics in the **healthcare** sector is matter of concern. Robots are devices that are unable to replicate the empathic capacities and reciprocity of human care relationships. Care robots, therefore, should only be used for care tasks requiring no emotional, intimate or personal involvement. If not used under certain framework conditions, robots can undermine human dignity.

#### 4.6 Privacy

4.6.1 **Facial recognition** compares someone's facial profile with a database to see if the scanned person appears in that database. It is used in police investigations or for security cameras in public spaces and its use is regulated by law. Such highly sensitive information must be stored safely and securely. Facial recognition, however, will become cheaper and easily accessible to all, for any shop, business or even private individual to use. There are attempts to use these techniques even for emotional recognition. The fear is that facial recognition technology could ultimately lead to a situation where it is no longer possible to walk down the street or go

shopping anonymously. The EESC demands that people have the right to be private in public spaces too. In general, camera recognition, without the knowledge of the people being observed, must be prohibited.

- 4.6.2 While the big brother scenario, where a government is spying on everyone, is already well known, the **little brother** scenario, where individuals or small companies are spying on each other, is becoming an ever greater possibility. For example, smart glasses can be used to record and retrieve data about an interlocutor or visitor. Other electronic spying gadgets will appear as advanced and affordable technology is further developed. The EESC emphasises that beyond the present GDPR, we need clear, strict rules to safeguard people's privacy.
- 4.6.3 With more **home automation**, the home, considered private, is becoming more transparent. The distinction between home and the outside world is blurring, as the walls no longer protect a house from prying eyes. Entertainment devices, alarm systems with security cameras and central control systems (desktop computer, smartphone, smart speaker) provide a range of entry points for hackers. The EESC calls for EU coordinated action to inform consumers about these risks and provide support for security measures.
- 4.6.4 One risk of digital systems lies in their complexity. In particular, the individual **consumer**, who does not have professional digital skills, needs strong support. For example, user manuals for digital equipment can be very long. They normally warn the user about privacy issues, but permission to use certain data is often given unwittingly, because people are not able to understand the entire manual or are suffering from so-called **consent fatigue**, due to the many times they have to grant permission to use their data to devices that capture data. This raises the question of where the responsibility lies in this process. The EESC calls for simplification and proposes to introduce EU standard procedures or standard privacy packages which are easy to understand for all.
- 4.6.5 The issue of privacy also applies to **digital platforms**. Platforms can easily track their users with simple tools. For example, Uber employees have been using the company's God View tool to track politicians, celebrities and others, something that has been stopped after a court case. The technology, however, still captures tracking and connecting data. The EESC is convinced that privacy can only be guaranteed through additional measures: restricting access to sensitive data to only a limited number of certified persons. Such security measures must be developed to the highest, most trustworthy standards, including regular verifications by independent EU bodies.

#### 4.7 **Work of the future**

- 4.7.1 Work will remain the central source of income in the digital age. Employability from an employer's perspective and the ability to work from an employee's point of view are two sides of the same coin in the digital transformation. The adaptability of employees to new tasks is equal to the possibility of adapting the work by digital technology to individual work requests. As the line between working to earn money and working for private purposes becomes increasingly blurred, the social partners in particular are being challenged to find and set new criteria for measuring individual performance in a fair way. Anticipation of digital change

requires involvement of employees through information, consultation and participation. Social security, public services of general interest and the safeguarding of ecological livelihoods remain prerequisites for the future working society in the digital transformation.

- 4.7.2 **Automation and robots** will have a significant impact on the future of work. For example, the use of driverless transport systems (DTS) is already commonplace for transporting materials in warehouses. Robots can also replace monotonous, heavy or dangerous work and a new generation of so-called "collaborative robots" can become physical partners for workers, particularly helpful for people with physical disabilities. Present-day robots mainly replace manual work, but robots using AI will also perform intellectual work. A significant number of professions will be affected, as robots take over certain tasks or even replace completely human workers, as we have witnessed in past decades. It is estimated that employment in all industrial sectors will remain stable until 2022. A look at large companies even shows that the shift in the division of labour between man and machine has created almost twice as many new jobs and functional roles as it has usurped. The EESC has discussed these issues a number of opinions<sup>7</sup>.
- 4.7.3 Uneven access to new digital technologies and a skills gap can be a source of gradually growing **differences in regional development** with impact on economic, cultural and, consequently, social development of those regions. The EESC calls for assessing the scale of possible social inequalities and its possible effects on the EU's integrity.
- 4.7.4 **Workers** collaborating or interacting with automated systems, or working with a large amount of information, may face certain problems. They must deal with complex information-intensive tasks. Virtual reality, for example, is used for training and planning purposes, while augmented reality supports maintenance projects. The EESC recommends, whenever new automation systems are planned in industry and commerce, using objective scientific methods to optimise and evaluate human-machine interaction.
- 4.7.5 **Employers**, on the other hand, are faced with the challenge of selecting suitable digital solutions from the wide range of new technologies. It is important to develop suitable technological assistance systems for companies' activities and work processes. Before introducing new technologies, it is also recommended to determine the technological competence of employees and, if necessary, offer training. The participation of employees in introducing new technologies is also a key factor.
- 4.7.6 The research area of **cognitive ergonomics** is making an upswing in the age of digitalisation. The scientific methods of **cognitive ergonomics** make it possible to objectively assess mental demands while dealing with new technical assistance systems. It combines different research disciplines, such as psychology and ergonomics, to evaluate user interfaces. The goal is an optimal workplace design and a win-win situation for employees and employers. In such a win-win situation, employees achieve an optimal level of job satisfaction, well-being and health and provide the company with optimal long-term performance and productivity. The EESC recommends that such evaluation methods become standard, for the benefit of employees and companies. The digital transformation should be monitored through comprehensive and

---

<sup>7</sup> [OJ C 434, 15.12.2017, p. 30](#); [OJ C 434, 15.12.2017, p. 36](#); [OJ C 237, 6.7.2018, p. 8](#), [OJ C 367, 10.10.2018, p. 15](#).

European funded work-oriented research into "digitalisation for the benefit of decent work". The EESC is convinced that only with efficient and employee-friendly design of Industry 4.0 systems will digitalisation be successful in the long term.

Brussels, 20 February 2019

Luca JAHIER

The president of the European Economic and Social Committee

---