European Commission

#EthicsGroup_EU

DEMOCRACY

in the digital age

European Group
on Ethics in Science and
New Technologies

ege

Research and Innovation

European Group on Ethics in Science and New Technologies
Democracy in the Digital Age

European Commission
Directorate-General for Research and Innovation
Unit 02

Contact Jim DRATWA
Email EC-ETHICS-GROUP@ec.europa.eu
RTD-PUBLICATIONS@ec.europa.eu
European Commission
B-1049 Brussels

Manuscript completed in June 2023.

This is an EGE Opinion, written and adopted by the members of the EGE: Nikola Biller-Andorno, Maria do Céu Patrão Neves (Vice-Chair), Migle Laukyte, Paweł Łuków, Pierre Mallia, Fruzsina Molnár-Gábor, Thérèse Murphy, Herman Nys, Laura Palazzani, Barbara Prainsack (Chair), Nils-Eric Sahlin (Vice-Chair), Tamar Sharon, Jeroen van den Hoven, Renata Veselská, Takis Vidalis.

PDF ISBN 978-92-76-99773-3 doi:10.2777/078780 KI-09-23-065-EN-N

Luxembourg: Publications Office of the European Union, 2023

EUROPEAN COMMISSION

European Group on Ethics
in Science and New Technologies

Opinion on

Democracy in the digital age

Opinion no. 33
Brussels, 20 June 2023

2023 Directorate-General for Research and Innovation

Table of contents

EXECUTIVE SUMMARY

PROTECTING **DEMOCRACY** IN THE DIGITAL AGE REQUIRES MORE THAN FIGHTING ELECTION MEDDLING, AND MORE THAN A NARROW FOCUS ON TECHNOLOGIES.

A WIDE AND DEEP UNDERSTANDING OF DEMOCRACY

Democracy is the form of government that is best suited to realise **fundamental rights and values**. It is itself a **set of values that enables people to live and thrive together** in solidarity.

CHALLENGES

Algorithms and social media provide powerful means for **manipulating opinion and public debate in the digital space**.

The **increasing reliance on tech corporations** for the provision of public services limits spaces of democratic control.

Socio-technical developments are too often driven by the interest in profit of a few, and not by the interest of society in the common good.

RECOMMENDATIONS

Stronger support for public participation, civic education, critical digital literacy and inclusive digital citizenship.

Coherent, impactful regulation for digital practices that serve all. Technology design for values and democracy.

Better support for civil society organisations & media professionals.

Publicly funded innovation to benefit the public – and basic needs safeguarded from market rationales.

EU diplomacy for protecting democracy and voicing civil society's calls for people and planet.

An understanding of privacy that does not treat it merely as a negative right but also as an individual and collective right to develop and express ourselves without being continuously watched and judged.

PREAMBLE

Democracy is in peril. Recent years have seen profound challenges to it, including the spread of misinformation, disinformation and otherwise misleading information (all of which we subsume under the label 'harmful' information[1]). Together with other injustices, they increase political polarisation and populism[2] and they widen inequalities, thus jeopardising democracy. Certain configurations of digital technologies contribute to these challenges, even if they are not their sole cause. At the same time, other ways of using digital technologies may help us to address some of these problems.[3] For example, digital voting, while making it easier for some people to vote, can also produce formal or informal barriers for those who are less digitally literate, or who have limited digital resources.

A democratic system can become an empty shell if it is not underpinned by fundamental rights and the values it seeks to protect and promote, such as justice, equality and solidarity. Because the challenges to fundamental rights and values have significantly changed since the paper age, the digital era requires new ways to understand and protect them. For example, it is now more than ever necessary to understand privacy not just as a negative right to be free from unwarranted interference in one's life, but also as a positive right, possessed by each of us, to develop and express our personality without being datafied or watched.

To protect democracy in the digital age, we need not a thin, but a 'thick' conception of it. This demands that democracy be understood from an ethical perspective. It is not just a political regime but also comprises a set of values that shape human behaviour and form the foundation of society. Respecting democracy in the digital age, then, requires much more than fighting election meddling, and more than a narrow focus on technologies. It requires ways of seeing, and standing up to, other digital harms. It also requires that, as a political union of 27 Member States with 24 official languages, the European Union harnesses the best that digital technologies have to offer in order to protect and strengthen the rule of the people in a deep sense, and to create mutual trust among all people living in the European Union, a true community of values and civic engagement.

It is against this backdrop, at the request of the President of the European Commission, that the European Group on Ethics in Science and New Technologies

[1] There is currently no agreed upon typology of harmful information; see Lesher et al. 2022.

[2] We understand populism as politics that pits the supposedly 'pure people' against a corrupt elite (see Mudde & Kaltwasser 2017). It undermines the core idea of representative democracy by waging attacks against democratically elected representatives of the people, which populists lump together with governments and other political elites that supposedly serve only particularistic interests.

[3] For the domain of health, the Lancet & Financial Times Commission on Governing Health Futures introduced the notion of digital determinants of health. This notion conveys not only that the use of digital tools, data and information shapes how people can protect, learn about and act upon their own health, but also that the digital practices of some people can affect the rights and interests of others (e.g. Kickbusch et al. 2021). Analogous to this, the notion of digital determinants of democracy could be used to highlight that digital practices affect how people understand themselves and how they act, but also that the digital practices of one group can have bearing on the interests and rights of others.

(EGE) [4] developed this Opinion on *Democracy in the Digital Age*. While it comes in the context of the European Commission revising the European Democracy Action Plan and preparing a Defence of Democracy package, this EGE Opinion also explicitly looks beyond these parameters. It is also set in the wake of the EGE's democracy statement of June 2021, *Values for the Future*, issued in the context of the Conference on the Future of Europe and delivered to the President on 9 June 2021.

The present Opinion addresses the safeguarding of democracy in a digital age, including, but not restricted to, free and fair elections. It looks at the role of online platforms, politics, media, civil society organisations, universities and other actors in opinion-shaping, including where malign foreign interference is involved. It discusses the relationship between policy measures that regulate civic spaces (e.g. to curb the spreading of harmful information), on the one hand, and fundamental rights safeguards on the other. Taking stock and looking towards the future, it also explores the role that digital technologies can play in developing better civic spaces and enhancing participation. In doing so, it emphasises the role of the European Union and everyone therein in protecting democracies. Last but not least, it addresses the problem of democratic governments losing their grip on basic public functions and the provision of public goods as these tasks are diversely and increasingly left to private actors.

This Opinion is organised in four main sections. The first introduces notions of democracy and examines the interplay between democracy and technology. The second examines known risks for democracy as well as what the EU has done to date to protect democracies in the digital age. The third section discusses new challenges, and the fourth looks at what could be done to address them. The Opinion concludes with a set of recommendations.

[4] The EGE is the independent multidisciplinary body appointed by the President of the European Commission that advises on all aspects of Commission policies and legislation where ethical, societal and fundamental rights dimensions intersect with the development of science and new technologies. The EGE's most recent outputs include its Statement on "*Values in Times of Crisis*" (November 2022) and its "*Statement in support of Ukraine*" (March 2022). Over the past years, it has also worked on matters such as artificial intelligence, the coronavirus pandemic, the future of work, genome editing, agriculture, energy, synthetic biology, security and surveillance, and the role of values in policy making.

1. INTRODUCTION: TOWARDS A 'THICK' CONCEPTION OF DEMOCRACY IN THE DIGITAL AGE

1.1. Democracy: Thick v. thin conceptions

'Democracy' refers to a form of government in which power lies with the people.[5] Beyond this minimal definition, there are many conceptions of democracy, signalled by qualifiers and adverbial prefixes: democracies can be representative, direct, parliamentary, associative, liquid, guided, socialist, deliberative, contestatory or agonistic, to give just a few examples (Alonso 2011, Reilli 2018, Strøm et al. 2003, Hirst 1996, Bader 2001, Blum & Zuber 2016, Brown 2001, Muldoon & Booth 2022, Mouffe 2000, Landemore 2017, Shapiro & Macedo 2000, Paxton 2019).[6] Most of these definitions share certain features. They contain, under different labels, the following elements: franchise, scope and authenticity (Dryzek 1996); a political system for choosing and replacing the parliament (and government) by means of free and fair elections; the participation of citizens in all aspects of social, political and economic life; human rights protection, the rule of law and safeguards and guarantees of the equitable and fair application of laws and procedures to all citizens.[7]

The EGE subscribes to a 'thick' conception of democracy. Democracy is the form of government underpinned by, and best suited to protect, fundamental rights as well as the values that these defend and promote, such as justice, equality and solidarity. Such a rich understanding of democracy helps to prevent democracy from turning into a kind of "phantom democracy" (Boggs 2011, Keane 2017) that has the outer form of a democratic system but does not substantively incorporate the rule of the people and the protection of their interests.

Our 'thick' conception implies that majority rule is not an end in itself. Instead, it serves the purpose of ensuring that as few people as possible live under a government that they have not elected (Kelsen 1920). Thus, the majority principle serves to realise and protect other substantive values and it is incomplete without the protection of minority rights.

A thick conception of democracy also entails a civic consciousness of engagement and the recognition of social, political and economic equality in society. It entails an understanding, on the part of everyone, that 'we are in this society together' – a sense of community and solidarity. Thick democracy thus requires more than the mere acceptance that others may end up benefitting more from widely shared principles of distributive justice. It requires civic solidarity and reciprocity that support just outcomes.

---

[5] The etymology is *dēmos* (the people) and *kratia* (power, rule).

[6] Recent additions include Norton's (2023) "wild democracy".

[7] Narrow definitions of citizenship can of course restrict the range of 'the people' to a much smaller group than those who permanently reside, and have a stake, in a country. For an understanding of "deep" democracy, see e.g. Walby (2009).

The digital transformations of recent decades have in some ways made it easier, but in other ways harder, to protect democracies. Digital technologies have created new arenas for exchange and democratic participation, but they have also altered the distribution of power, both globally and within countries.[8] Foreign governments, private enterprises, and even rich individuals can interfere with elections more easily, manipulate public opinion,[9] or spread harmful information across the globe. The latter has been found to have a direct effect on fundamental rights (European Parliament 2021a). This is not, of course, a linear process in which technologies cause the problems that then, in turn, require better technologies to fix them. The risks and benefits of digital technologies are shaped by the way they are designed and regulated, and by the ways in which we use them. In this way, they are influenced also by dominant values shared in a given society.

We shall argue in this Opinion that the strengthening of democracies in the digital age requires three things. First, digital technologies need to be regulated in such a way that they serve people and communities, instead of merely benefitting a small political and corporate elite at the cost of most others (see Sections 2 and 3).

Second, it is necessary to reconsider how we can best protect the ethical values that underpin democracies, including autonomy, justice, solidarity, equality and non-discrimination. For example, in the era of grave power asymmetries between individuals on the one hand and companies and other corporate data users on the other, 'consent' to data use is often a precondition for access to (sometimes even public) goods and services. In this context, we cannot assume that people 'freely' agree to their data being used by others (see Section 2).

Third, autonomy and the self-determination of individual people and of entire populations are compromised by the fact that democratic governments are losing their grip on basic public functions and the provision of public goods as these are increasingly left, wholly or in part, to private entities. This needs to change (see Section 3).

In all this, it must be borne in mind that the online world is structurally different from the offline world, in terms of network size and topology, and in terms of the quality of connections between people, and between users and providers. In the online world, weak ties between people typically dominate over strong ties. Often, there are no cues indicating epistemic quality of information. Democratic corrosion is exacerbated by key features of the attention and platform economy, with its reinforcement architectures, techniques of personalisation and audience segmentation, manipulative targeting, and ubiquitous choice architectures with built-in nudges and dark patterns.[10] The rapid advancement of artificial intelligence

[8] Many low-income countries are placed at a disadvantage by the fact that corporations carry out business on their territories but pay taxes in the high-income countries where they are headquartered. Moreover, as noted by Törnberg (2023: 5), digital "platforms' disruptive strategies have proven particularly efficacious in countries in the Global South", where poorly resourced public institutions have provided "conditions favourable to laissez-faire platformization. Labor platforms such as Uber feed on neoliberal conditions not only to lax regulation, but also as they depend on a pool of desperate workers" (see also Chueri 2022).

[9] An example is the use of bots to create the illusion of public support; e.g. Savaget 2019.

[10] Dark patterns, also known as deceptive design patterns, are different interface design choices that push users to behave in ways that are detrimental to their interests.

(AI) is already altering production and distribution of information with, so far, little knowledge about the consequences of large-scale use of AI. Many agents seek to benefit personally from this situation. Some try to present fake or problematic evidence as 'science', or use science in manipulative ways. Influencers and meddlers compromise independent journalism with fake news, propaganda and hyper-partisan narratives. Lobbyists have undermined trust in politics. Profit maximising and managing elites have obliterated trust in the financial sector and the corporate world, and "conspiracy entrepreneurs" (Rosenblum & Muirhead 2019) crowd out serious attempts to understand the world.

At the time of writing, for example, ChatGPT and other Large Language Models seem to be taking society by storm. As educators, journalists, coders and other professionals scramble to develop guidelines on how to integrate this technology in their work practices, we are confronted with a social experiment of extraordinary scale, which includes risks to democracy. AI bots can produce abundant new sources of misinformation, reproduce harmful and biased content, lead to privacy infringements, and cause important environmental costs (Bender et al. 2021; Marcus 2022). We can question how prepared our societies are to deal with a technology which convincingly passes off as a speaker of truths, while it has no intentionality, agency, meaning-making capacity, or ability to be held accountable (Bender 2020; Weil 2023). A wide societal deliberation is needed to ascertain if and which such sociotechnical arrangements are desirable; if so, they must be designed with commonly agreed values.[11]

1.2. Threats to democracy and the involvement of digital practices

Democracy and the fundamental rights, that both support it and are supported by it, are under serious threat. Foa and Mounk (2017), for example, speak of a "de-consolidation" of the entrenched democratic order in the western world that is taking place at the beginning of the twenty-first century. Autocracies, oligarchies and other non-democratic regimes are on the rise. Some are evolving as a result of decline in existing democracies, as happens when populism is growing. Such regimes incorporate democratic elements into what are, in effect, hybrid political systems. They lack free and fair elections, universal suffrage, judicial independence, a free press and other human rights protections (e.g. Heckelei, 2016; Brown 2001), yet they are sold by their leaders as the 'true' will of the people. Populists celebrate such autocratic systems as a 'purer' form of democracy, pitting 'the people' against 'the elites' (Mudde & Kaltwasser 2017). In *How Democracies Die* (2018), Levitsky and Ziblatt argue that the "tragic paradox of the electoral route to authoritarianism is that democracy's assassins use the very institutions of democracy – gradually, subtly, and even legally – to kill it" (p. 8). One of the biggest risks in the twenty-first century is that we continue to trust democracies when they have stopped functioning as such (Runciman 2018).

[11] See the EGE Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems (EGE 2018).

The features of the democratic state that have declined most rapidly across the globe in recent years are 'trustworthy independent media', 'freedom of expression' and 'access to alternative sources of information' (e.g. Gorokhovskaia et al. 2023; Reporters Without Borders 2022; IPSOS 2019; Hanitzsch et al. 2018). In each case, the decline is, in part, a consequence of the growing influence of digital media. To give just one example, they make it hard for independent, professional journalism to obtain sufficient funding, and therefore shift power to those who own and control online media and platforms.[12] Against this backdrop, there is an urgent need to examine what democracy means, and what we want it to mean. It is not enough to hold onto an empty shell.

1.3. The role of ethics

Ethics as a systematic and critical description, analysis and justification of moral claims and moral considerations helps us to shape institutions, policy, technology, laws and governance in a digital age. Taking democratic values seriously in the European Union requires that we recognise ethics as a source of legislative choices that can help to critically evaluate them – but which is not an alternative to them.

The EGE has described its views on the role and the future of moral values in more detail in its Statement "Values for the Future: The role of ethics in European and global governance" of June 2021 (EGE, 2021). In this context, the pitting of regulation against self-regulation and ethics (something currently being seen in connection with AI ethics, for example), is a dangerous development (Van Dijk et al. 2021; Yeung et al. 2020). In the recent past, attempts have been made to relegate ethics to self-regulation, to give it a bad name as an obstacle to innovation, and defund research in the social sciences and humanities (e.g. Wagner 2018; Sides 2015; Pinker 2015; Gibbons 2020; Taylor 2009). At the same time, it has become very clear that we cannot make the fundamental ethical problems and hard questions of advanced digital societies go away by obfuscation and avoidance. They are questions about how we (want to) live and what society we (want to) live in. The answers we give to them will determine what kind of society our children will live in.

EU institutions are known for the attention given to ethics across, for example, innovation, foreign policy, finance and health. Indeed, we need to make fundamental values the basis for and justification of choices that societies as a whole make in order to prosper, live in peace and freedom, and ensure that even the most vulnerable in our communities are treated with respect and consideration. The design of novel forms of (digital) democracy is one of the main routes to achieve a Europe that reaches the moral ideal it projects internationally and defends with vigour.

[12] At the same time, it should be noted that some studies found a positive association between digital media use and participation in civic and political life (Boulianne 2020), especially in emerging democracies and autocracies (Lorenz-Spreen 2022).

2. THE KNOWN RISKS FOR DEMOCRACY AND THE EU MEASURES THAT SEEK TO ADDRESS THEM

The EU's commitment to democracy has a long history. Schuman's definition of democracy considers Europe "the embodiment of a generalised democracy [and] what characterises a democratic state are the objectives that it sets and the means it deploys to attain them. Democracy is at the service of the people and works in agreement with it" (Schuman 1964). Article 2 of the Treaty on European Union (TEU) identifies the values that constitute the essence of a system of freedoms and a community of values, i.e., a democratic society, and declares them to be the starting point of the EU (see also European Declaration on Digital Rights and Principles for the Digital Decade, 2022). These values include justice, equality and solidarity, as well as respect for the fundamental rights that enforce them. The integration, legitimation, material content and functioning of the EU are conditioned and determined by these values. The EU has made these values Europe's *raison d'être* – a purpose that all Member States are also expected to continuously contribute to building, supporting and strengthening.

Values that guide decision-making as benchmarks require concretisation in rules. The EU has powerfully advanced such concretisation in recent years with regard to the EU-specific concept of democracy, which at the same time rests on the obligations of the Member States under international law (cf. only Art. 3 of the 1st Additional Protocol to the European Convention on Human Rights (ECHR)). These democratic values are explicitly mentioned in legal instruments such as the TEU, and the EU Charter of Fundamental Rights (CFREU). They appear regularly, also, in secondary law, and are binding for EU organs, Member States and citizens. In that sense, they form the basis for any legitimate interest, public or private, in the EU. Any individual right or obligation, and any institutional competence, must ultimately be grounded in them.

2.1. What are the known risks?

2.1.1. Harmful information, polarisation and lack of transparency

The EGE agrees with those who have publicly expressed concern about the unfavourable knowledge conditions and power relations of the digital age (e.g. Kickbusch et al. 2021). If the public sphere, and the basic standards of public reason, are not meaningfully oriented towards appropriate epistemic values and intellectual virtues, this shared public sphere and its robust conceptions of community and solidarity will suffer in various ways. In the words of Shoshanna Zuboff:

> On the strength of their surveillance capabilities and for the sake of their surveillance profits, the new empires engineered a fundamentally anti-democratic epistemic coup marked by unprecedented concentrations of knowledge about us and the unaccountable power that accrues to such knowledge. (Zuboff 2021)

This is reminiscent of the observation that "a people that no longer can believe anything cannot make up its mind. It is deprived not only of its capacity to act but also of its capacity to think and to judge. And with such a people you can then do what you please" (Arendt, 1974).

Dialogue and deliberation are essential in a robust democracy.[13] Jürgen Habermas famously referred to the 'public sphere' as the place where public opinion is formed (Habermas 1989; 2022; Thiel 2023). That sphere has several key characteristics. First, it is a place where people come together as citizens, and not as representatives of particularistic or corporate interests. Second, there is no power behind these exchanges between citizens that intimidates them, or otherwise coerces the deliberation in a specific direction. The deliberation taking place in the public sphere, according to Habermas, has an important democratic function as a corrective to, and controller of, the everyday functioning of the state. Cafés – insofar as they do not exclude anyone, such as women, economically deprived groups, or minorities – have been considered archetypal places of the public sphere: places for social interaction and deliberation between the private sphere and the sphere of public authority (Calhoun 2012; Steiner 2015).

Habermas' ideal of the public sphere has been criticised (e.g. Fraser 1992) as unrealistic, and more importantly as an ideal that ignores the realities of life for marginalised groups. Still, even as a flawed ideal, Habermas' portrayal of the public sphere helps us to pinpoint particular challenges that have emerged in the digital age. Today, when much of the public sphere is online, for example on social media platforms, the owners of most of these platforms benefit from hate and division.[14]

---

[13] The Committee for Bioethics of the Council of Europe (DH-BIO at the time, now CDBIO) issued an important 'Guide on public debate on human rights and bioethics' (2019).

[14] In his more recent work, Habermas (2022) considers platforms the main organisational form of digital communication. He draws upon Zuboff's (2019) depiction of surveillance capitalism and emphasises that algorithmic personalisation is detrimental to an inclusive public sphere.

The wilder the lies, the more outrageous the defamations and the more compelling the conspiratorial tales, the longer many people seem to stay on the platforms,[15] driving up revenue.[16] As recent scandals over voter manipulation[17] and incitement to racialised and sexualised violence illustrate, the platforms – although they portray themselves as neutral 'infrastructures' that cannot be held responsible for the content shared – can be paid to serve the interests of powerful political and economic actors (e.g. Leetaru 2018; Kofman & Tobin 2020; Sapiezynski 2022; Tech Transparency Project 2023; Ali et al. 2019; Chandwaney 2020; Hinds et al. 2020). The more private corporations take over public functions, the more public spaces become opaque, unequal and at times outright dangerous.

There are also risks stemming from how people use platforms as a news source. When fewer people obtain their news from independent quality-controlled media and more do so from social media platforms, a people's shared information reality is narrowed. It is split into ever smaller and more fragmented groups of like-minded individuals as the platforms' algorithms identify groups of people who display similar behavioural patterns (e.g. 'likes' on websites and social media, or purchase data) and target them with tailored information that may be 'relevant' and 'interesting' for them (e.g. Cinelli et al. 2021). The consequences may be that people are less exposed to information about realities that are different from theirs, making it harder for them to relate to diversity as such; and that they may end up with a skewed understanding of reality and assume that others think and act like them. We are witnessing a structural power shift from transparent, non-monopolistic public spaces to unaccountable, profit-driven spaces that can be changed, closed or used for idiosyncratic purposes at the will of a few powerful actors (see also Section 2.2.3.).[18]

In this light it is urgent to ensure the protection, safety and empowerment of journalists and other media professionals,[19] and to acknowledge the important role of think tanks and other civil society organisations in promoting reflective and

---

The plebiscitary public sphere of social media platforms inflates "a sphere of communication that had previously been reserved for private correspondence" (2022: p. 166).

[15] There have been manifold studies in this regard. Some studies suggest, for example, that conservative and right-wing audiences are more vulnerable to harmful information (e.g. Baptista & Gradim 2022, Freelon et al. 2020, Frischlich et al. 2021, Zhuravskaya et al. 2020). Other research found that people over 65 are seven times more likely to share fake news than younger individuals do (European Parliament 2019).

[16] The European Parliament, in its *Resolution on online platforms and the Digital Single Market* (2016/2276(INI)), adopted in June 2017, called upon the Commission to analyse the latest developments and legal framework as regards *fake news*, and the possibility to introduce legislation to counter the dissemination of this content. The European Council addressed the matter once again in March 2018 (European Council meeting of 22 March 2018 – Conclusions) to highlight the responsibility held by social media networks and digital platforms in securing transparent practices and the full protection of citizens' privacy and personal data.

[17] E.g. European Parliament (2021b) on a "next generation repression toolkit" which refers to practices and technologies that are very difficult to detect.

[18] European Parliament, 2019, Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States.

[19] Commission Recommendation (EU) 2021/1534 of 16 September 2021 on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union.

informed political debate. Strengthening media and improving journalism standards includes the making available of sufficient public funding, support programmes for investigative journalism and for improving fact-checking services and credibility indices.[20, 21]

2.1.2. Unintended effects of an unduly narrow understanding of privacy

It has been argued that the increasing datafication of people's lives and bodies – i.e. the growing capture of specifically human practices and characteristics in the form of digital data of various kinds – has changed the way people understand privacy (Surden 2007, Friedewald et al. 2017). This does not mean, however, that people care less about privacy. Privacy remains important, but some have become resigned to the fact that they must surrender certain privacy rights to obtain access to services and tools they need in daily life (Turow et al. 2015). Many have given up the hope that their privacy can be fully and effectively protected in today's world. Moreover, we cannot ignore the fact that the information describing what one is consenting to when one 'accepts' a website's privacy policy is unduly long and technical, and incomprehensible to many people. From this perspective, it could be said that the current consent system functions more as a waiver of responsibility for those who obtain data than as a reinforcement of the right to privacy.

Many of the larger technology companies are notorious for their questionable privacy policies and data sharing practices. TikTok, for instance, was banned by EU institutions and prohibited for use by public sector employees in the course of their work in different countries (Xu et al. 2023). And Google continues paying fines for privacy infringements in the EU.[22] While the sharing or re-selling of personal data

[20] European Parliament, 2019, Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States.

[21] In this respect, the EU is funding research projects under Horizon Europe (under the calls Media for democracy, democratic media and Politics and the impact of online social networks and new media).

[22] E.g. in France (https://www.cnil.fr/en/cookies-google-fined-150-million-euros, https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf, https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-orders-20-organisations-comply, https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf, https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf, https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en, https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf, https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf), in Sweden (https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en, https://www.imy.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf, in Belgium: https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu600000-fine-google-belgium-not-respecting-right-be_en, in Spain: https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/the-aepd-has-imposed-sanction-on-google-llc-for-transferring-personal-data-to-third-parties, https://www.aepd.es/es/documento/ps-00140-2020.pdf).

may be made legal by the terms and conditions of the digital services that users agree to, it remains ethically dubious, and constitutes a breach of what Helen Nissenbaum (2011) calls "contextual privacy". For example, when we share personal information on social media, or use our supermarket loyalty card, we do not expect the data to be used by, for example, the government. This runs counter to people's reasonable expectation of privacy.

In the digital era effective privacy protection needs to go beyond the protections set up in the paper age. It is no longer enough to ensure that individuals are asked for their consent before their data is used. 'Consenting' to data use has become a precondition for obtaining access to essential services, such as communication and news platforms, and sometimes even healthcare. This may be efficient for companies, but it is not effective as an *informed* choice, as assessing and communicating the risks of data processing is fraught with challenges. Privacy in the digital era must be understood as more than merely an individual's right to freedom from undue interference. It is, in addition, a positive right to have the space to develop and express oneself. In the words of Julie Cohen:

> Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops. (Cohen 2013: p. 1905)

In summary, privacy is not only valuable because personal data in the wrong hands can be used in ways that negatively impact a person's life chances – as when, for example, a health insurer raises your premium when they find out how much of your weekly supermarket budget is spent on potato chips, or a future employer decides against hiring you in light of your tweets about how you cope with a mental health problem. Privacy is the "breathing room we need to engage in the process of self-development" (Cohen 2013: p. 1906). It is a buffer that gives us the space to develop an identity that is separate from the judgement of others. It is crucial for us to manage these pressures, and to form an identity that is not dictated solely by social conditions.

2.1.3. Surveillance and discrimination by algorithm

Social and political theorists have been studying the chilling effects of surveillance technologies for decades. An awareness that one is being watched, they argue, changes people's behaviour (Friedewald et al. 2017). The gaze of the 'watcher' is internalised by us, the people, and comes to shape what we do, how we think and ultimately who we are. Surveillance curtails our autonomy. Today, it is *decentralised*, enabled by self-tracking devices, the internet of things and social media. It is no longer happening merely 'from above', but also horizontally, as we share information with others and monitor ourselves. It is also *ubiquitous*, in that it is not confined to the walls of the prison, or school, or hospital, but appears in many spheres of social life and all the time. The breathing room that privacy constitutes is

essential for democratic citizenship.[23] Privacy and related values are currently under threat by the constant data collection, profiling, nudging and prediction-based coaching that characterises the digital age.

A related problem is that algorithms and automated decision-making systems are increasingly being implemented in areas that are vital to the functioning of healthy democracies, including public administration (Van Bekkum & Borgesius 2021), law enforcement (FRA 2022), education (Bedingfield 2020), healthcare (Ledford 2019) and hiring procedures (Whittaker et al. 2019). While these systems are intended to improve efficiency and increase the 'objectivity' of decision-making procedures, they are trained on data which themselves include biases and prejudices that exist in our societies, and they thus inevitably introduce or reproduce these biases. Experience has shown that the decisions and recommendations that these systems produce often lead to discriminatory outcomes, typically towards already vulnerable groups in society, such as ethnic minorities, women and economically deprived groups (Eubanks 2018; Maki 2011; Boulambwini & Gebru 2018). Moreover, and as these systems become increasingly integrated in public sectors, people do not always have a possibility to opt out or seek redress for decisions that are made in highly untransparent, 'black-boxed' ways (Pasquale 2016).

In 2019, Philip Alston, the UN Rapporteur for extreme poverty and human rights, warned that there is a "grave risk of stumbling zombie-like into a digital welfare dystopia" (UN Rapporteur on extreme poverty and human rights 2019). A telling example of this is the recent childcare benefits scandal in the Netherlands, which revealed that algorithmic decision-making for fraud detection wrongly singled out parents with dual nationalities, often with migrant backgrounds (Amnesty International 2021). Asked to immediately pay back large sums of allowances that they had received, this has caused severe financial difficulties to a number of these families, including losing their homes and children being given into care facilities. To avoid such injustices, we must ensure that AI systems are not used in ways that undermine democracy, are discriminatory, or otherwise violate fundamental rights (see Section 2.2.3.).

2.1.4. Foreign interference

Another problem with digital surveillance is the opportunity it potentially affords for interference by private or state actors with interests in a foreign country (see also European Parliament 2019). An example is the development of malicious software deployed by private companies for the purpose of industrial espionage (see also European Commission 2019a).

It is crucial to consider measures to strengthen the resilience of democracies at a global and international level. Espionage, for example, is best addressed through

[23] We use the term citizenship to refer to a person's identity and roles as part of a political community. Holding citizenship status in the formal sense can be part of a person's role in a political community (as it determines their entitlements and obligations towards the state), but it is not a requirement for a person being a citizen in a wider sense. In the widest sense, citizenship requires that a person has a stake in the political community that they are part of.

public international law, by reference to the norms regulating the relation between states and state actors conduct – such as the principle of non-interference (Kunig 2008: recitals 1-6, recitals 22 et seq.), or the framework provided by diplomatic law – and human rights. In case of interference in foreign elections, in contrast, these frameworks are less immediately helpful, because such interference does not typically meet the legal requirements to be considered an intervention contrary to international law (Steiger 2021). This would only be the case if an election result was directly changed, election infrastructure was attacked, or violent unrest was provoked with the help of false news (cf. Kunig 2008). Other, equally harmful inferences do not fall under the non-intervention principle.

When a political group, party, or a government pays a social media platform to show certain types of information to a specific group of people in order to steer their election behaviour, for example, this can represent a violation of the political independence of a state as part of its sovereignty (e.g. Federal Government of Germany 2021, UN Working Group on developments in ICT in the context of international security 2021; UN Office for Disarmament Affairs[24]). Some countries consider state sovereignty in cyberspace to be a rule of international law that can be deemed violated in its own right. Internally, sovereignty allows states to regulate matters relating to cyberspace independently. Externally, it guarantees both the territorial integrity of states and their political independence. Political independence, as part of sovereignty, would then be independently violable. The preconditions for a violation are often disputed. In particular, it is currently unclear whether it would be necessary to exceed a materiality threshold, as in the area of territorial integrity, in order to violate political independence (Schmidt 2021).

Regulating foreign interference will come with the challenge of integrating openness and international cooperation together with the protection of democratic systems and fundamental rights. As was reported by those developing the European Commission's Defence of Democracy package, identifying covert malign action might require efforts towards increased transparency and accountability in many areas, from social media platforms to news production as well as research and other organisations. Yet this must not come at the cost of weakening these institutions and people's freedoms and rights, many of them central to a thriving democracy, as civil society organisations have stressed (e.g. Civil Society Europe & Philea 2023; Wheaton & Goujard 2023). Regulatory efforts against malign foreign interference, and their enforcement, should not undermine the fabric of trust and togetherness in societies; they should seek to uphold and safeguard our values and the institutions built on the basis of these values. Particular attention is required in relation to unintended consequences of measures, and to measures which would risk being instrumentalised and abused – a form of 'dual use' – to stifle democratic life. Constructive proposals that have been made include the establishment of a protection mechanism for the reporting of attacks and increased support for organisations to better monitor the use of EU funds (Civil Society Europe & Philea 2023). Such measures would, for example, empower civil society in protecting its organisations.

[24] https://www.un.org/disarmament/ict-security/

2.2. What is being done to protect and strengthen democracies in the EU

2.2.1. Legal efforts

A "new push for European democracy"

The European Commission has already taken firm action to promote robust democratic processes within the EU. It has introduced extensive regulation and policies in support of democracy, the rule of law, fundamental rights and core ethical principles.

Securing free and fair elections and protecting democratic processes has been at the heart of the European project. The European Commission has reinforced these efforts with its electoral package of 2018,[25] giving them priority status.[26] They were integrated, as part of President von der Leyen's 'new push' for European democracy, into the initiatives announced in the 2020 European Democracy Action Plan (EDAP).[27] The EDAP has the aim to "empower citizens and build more resilient democracies across the EU by (a) promoting free and fair elections, (b) strengthening media freedom, and (c) countering disinformation".[28]

In 2021 the Commission adopted a package of measures to reinforce democracy and protect the integrity of elections. This included a Communication, a legislative proposal on transparency and targeting of political advertising, two legislative proposals on the right of EU citizens residing in a different Member State to vote and stand as candidates in elections to the European Parliament and municipal elections, and a legislative proposal to update EU rules on the funding of European political parties and foundations. It also issued the European Media Freedom Act[29] and several actions to support the strengthening of the rights and safety of journalists.[30] The proposals for a regulation on the transparency and targeting of political advertising and the regulation on the statute and funding of European political parties are currently under negotiation among the European co-legislators.

---

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0637&from=EN

[26] The implementation of the electoral package was reported on in the Commission's report on the 2019 European parliamentary elections: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0252

[27] https://commission.europa.eu/document/download/e0f68623-24f9-45ce-a784-62ad2e786db1_en?filename=edap_factsheet8.pdf

[28] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

[29] https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5505

[30] https://ec.europa.eu/commission/presscorner/detail/en/fs_22_2653, https://digital-strategy.ec.europa.eu/en/library/recommendation-protection-safety-and-empowerment-journalists-factsheet

Other measures that have been taken forward include the work in the framework of the regular meetings of the European cooperation network on elections,[31] such as a *Joint mechanism for electoral resilience* organised and coordinated through said network in cooperation with the Network and Information Systems (NIS) Cooperation Group and the EU's Rapid Alert System. Having started its operations in 2022, this mechanism's primary operational focus has been to support deployment of joint expert teams and expert exchanges with the aim of building resilient electoral processes, in particular in the area of online forensics, disinformation and cybersecurity of elections, providing direct support to national entities.

In her 2022 State of the Union address, President von der Leyen announced an initiative to defend democracy from malign foreign influence. At the time of writing, this Defence of Democracy package is due to complement actions already taken at EU level under the EDAP, with a focus on transparency measures to prevent covert foreign interference. It is also meant to include specific measures on electoral matters ahead of the elections to the European Parliament, and measures to foster an enabling civic space and promote inclusive and effective engagement by public authorities with civil society organisations and citizens. Further, it is also supposed to take into account several democracy-related proposals made by the Conference on the Future of Europe as regards citizen engagement in policy making. It has been communicated that it will be consistent with the Rule of Law report,[32] the upcoming anti-corruption package and other measures to further increase transparency.

A European regulatory "digital strategy"

By closely linking EU values to fundamental rights, democracy within the Union also affects the way the EU institutions represent the interests of people living in the EU. The protection of privacy and personal data is an example of the EU's commitment to the prioritisation of people's interests: Whether and how personal data may be processed, whether by private companies or by public authorities, depends on the balancing of the processing interests with the interests in protecting the data. The EU General Data Protection Regulation (GDPR), which entered into force in May 2016, aims to secure a high level, general and uniform protection for personal data in all Member States through its direct applicability. The EU has given individuals considerable control over the way their data is used by granting them differentiated rights vis-à-vis those who control the data, in relation to different categories of data and processing situations. The intent is to avoid various forms of harm caused by the processing that limit the negative freedom of individuals (absence of external constraints), prevent them from presenting themselves freely to others, and exacerbate asymmetries of information and power between individuals and data controllers (Molnár-Gábor 2016). Unlike many other jurisdictions, the EU has regulated data protection both in a standardised manner, so that public and private

[31] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship/democracy-and-electoral-rights_en#european-cooperation-network-on-elections

[32] https://commission.europa.eu/publications/2022-rule-law-report-communication-and-country-chapters_en

actors are generally covered by the same legislation, and cross-sectorally, meaning that a set of general rules applies to personal data regardless of the processing context (healthcare, finance, marketing, etc.) in which it is used. Some contexts are subject to specific provisions or further legislation.

By seeking the enactment of legislation which cannot be circumvented by private agreements as a result of its fundamental rights character, the EU has eschewed private law solutions to the problem of data protection (European Commission 1998). Remedies for harms emerging from data use are limited to cases where the breaking of a law resulted in the harm – leaving without adequate support people who were negatively affected by legal, yet harmful practices (e.g. McMahon et al. 2020). Moreover, legal concepts such as public interest and trade-offs (e.g. related to the research privilege) have not been suitably addressed in their implementation and interpretation at EU level or in the Member States. While a margin can ensure fair and just application of the law in individual cases, efforts to harmonise the data processing rules can easily come to naught. Intermediate-level standardisation for sector-specific data processing (specific rules concretising GDPR rules in a sector-specific manner) through, for example, codes of conduct, have so far remained an unused option in many data processing contexts. Last but not least, the GDPR's mechanisms for international data transfers ensure that the obligations applicable under EU data protection law continue to apply after the transfer of data outside the EU and the European Economic Area, including the obligation on proportional balancing of benefits and harms. Concerns about fundamental rights in a third country, for example in the context of surveillance activities by public authorities, influences the assessment of the level of protection in that country, and lead to its rules being considered disproportionate, or even contrary to the essence of the fundamental rights concerned (CJEU C-362/14 2015; CJEU C-311/18 2020). If a European Commission assessment for a third country is not yet available, potential data transmitters must examine the entire legal system of third countries with regard to fundamental rights protection before making international data transfers to that country. This increases the complexity and compliance costs associated with conducting outbound data transfers from the EU and the European Economic Area to third countries.

In recent years, the European Commission has taken an active interest in digital transformation, drafting legislation in response to this rapidly changing field. In particular, the proposed AI Act (COM/2021/206 final), the Regulation on the High Performance Computing Joint Undertaking (COM/2020/569 final), the Cybersecurity Act (Regulation (EU) 2019/881), as well as the Directive on the European Electronic Communications Code (Directive (EU) 2018/1972) all respond to new technologies in the digital space.

The Digital Services Act (Regulation (EU) 2022/2065, DSA) and Digital Markets Act (Regulation (EU) 2022/1925), and the Data Governance Act (Regulation (EU) 2022/868, DGA) and its sectoral concretisations in, among other things, the health sector through the draft European Health Data Space Regulation (COM/2022/197 final), together with the Open Data Directive (Directive (EU) 2019/1024) and the proposed Regulation known as the Data Act (COM/2022/68 final), complete the EU digital policy scaffold. The last of these will form part of a cross-sectoral governance framework for access to, and use of, data. It will establish harmonised rules on matters affecting the relationships between actors in the data economy, including access to, and use of, data generated by the use of a product or linked service. In addition, it aims to facilitate switching between data-processing services and to

improve data-sharing services and mechanisms, and data interoperability in the EU (COM(2022) 68 final: recital 5 and 7 of the explanatory memorandum and Article 1(1) of the proposal).

It is expected that further legislation will be presented in the near future, including a revision of the Database Directive (Directive 96/9/EC), the proposed Regulation on Privacy and Electronic Communications (COM/2017/010 final - 2017/03 (COD), revision of the ePrivacy Directive) and the upcoming Cyber Resilience Act (COM(2022) 454 final). A legislative proposal to build an EU space-based global secure communications system has also been announced (COM/2022/57 final). The revised Database Directive will have a focus on facilitating the trading and sharing of machine-generated data, and data generated as part of the rollout of the internet of things.[33]

In summary, these legislative initiatives aim to improve fundamental rights protection in relation to digital practices. The goal is to inhibit encroachments on the rights of data subjects by preventing manipulative and exploitative practices associated with digital technologies as well as misuse. The regulations will seek to define an appropriate balance between the rights and interests of data protection and the goals of data processing more broadly, and to implement the results of this balance at a technical level through the realisation of principles of privacy-by-design and privacy-by-default (Regulation (EU) 2019/881, Art. 1(1) and recitals 1, 16, 41) – which means, in essence, that privacy-protecting solutions are designed into the hardware and the software. In order to develop and apply digital technologies in a way that respects and further promotes fundamental rights, the right to access data, including secondarily generated data, must be balanced with data protection, and the reuse of data (including public sector data) must be enabled in a privacy-preserving manner. The prevention of misuse and a strengthening of the proportionality of trade-offs are both based on risk assessment. They are therefore linked to the best possible preservation of the affected but competing values. Overall, digital technologies should serve enhanced fundamental rights protection, with due consideration of the additional vulnerability they create.

The regulations also promote the creation of a cross-sectoral framework for data governance. Ideally the framework will reduce fragmentation between data processing and the corresponding rules for actors, between different forms of access and use, and across regulatory areas. Harmonisation within the EU will be further supported by strengthening EU agencies like the Cybersecurity Agency (Regulation (EU) 2019/881) and promoting common data spaces in order to reduce regulatory fragmentation between Member States and promote technical and normative interoperability and competition between enhanced digital services while respecting fundamental rights. Establishing new digital market players such as data intermediaries (COM/2020/825 final: Art. 1 and recital 153) promotes rule implementation and enforcement within the EU and enables connectivity to EU-external data spaces. Harmonised rules for liability and due diligence could further promote standardised enforcement. Improved security and information assurance should promote privacy protection against spoofing and eavesdropping by third parties (COM/2022/57 final, Explanatory Memorandum: p. 9) and strengthen the EU as a data actor on a global scale.

[33] https://digital-strategy.ec.europa.eu/en/policies/protection-databases

Rules against discrimination

The obligation to respect the principle of non-discrimination is enshrined in Art. 2 of the Treaty on European Union (TEU), Art. 10 of the Treaty on the Functioning of the European Union (TFEU) (requiring the EU to combat discrimination arising on various grounds), and Art. 20 and 21 of the EU Charter of Fundamental Rights (CFREU) (equality before the law and non-discrimination based on a non-exhaustive list of grounds). In secondary law, the Equal Treatment Directive (Directive 2006/54/EC), non-discrimination laws (Directive 2000/43/EC; Directive 2000/78/EC; Directive 2006/54/EC; Directive 2004/113/EC; Directive Proposal COM(2008)462) and data protection laws are among the legislative instruments operationalising non-discrimination requirements. In Member States, 'equality bodies' implement and enforce the EU value of equality and defend the right to non-discrimination. These public organisations assist victims of discrimination and monitor and report on discrimination issues arising from legal obligations defined by the grounds of discrimination set out in EU law.[34]

Digital technologies, and in particular also machine learning and other practices commonly subsumed under the label of artificial intelligence (AI), can exacerbate or cause new instances of discrimination. This can be rooted in biased training data, or in the ways in which organisations define target variables and class labels (e.g. Zuiderveen Borgesius 2018). The most important rules operationalising the handling of AI in the EU based on fundamental rights and ethical values are set out in the proposed AI Act (AIA, COM/2021/206 final). In draft form, this Act contains obligations on such matters as data control, human supervision and a guarantee of the comprehensibility of AI decisions that are based on the risk of discrimination. The European Commission has already presented the draft of an AI Liability Directive, but this is limited to claims based on injury to life, health, physical integrity and property (COM/2022/496 final).

Where data is concerned, the obligations are limited to certain types of AI systems that are classified as high-risk applications (COM/2021/206 final: Art. 16 et seq.). For other, non-high-risk, AI systems only a low level of obligation applies. Even if the GDPR is fully applicable, the rights of data subjects reach their limits due to the technical nature of machine learning systems and the way in which they draw conclusions (Müller 2022). Accordingly, there is a need for improved protection for the rights of data subjects, especially regarding transparency obligations (Art. 52 AIA) and rights corresponding to user obligations in general (Art. 29 AIA) (Ebers et al. 2021). Clear definitions (e.g. of the concept of bias, the distinction between interpretability and explainability, and the level of transparency required) should be established. Until this happens the standardisation of AI systems – which is not only a technical but also an ethical-legal issue – will be left to private regulatory actors such as standardisation organisations (Ebers et al. 2021). The standardisation will not be discussed by society as a whole, and the corresponding decisions will not be made through democratic processes. A lack of democratic legitimacy and the limited influence of relevant interest groups on standardised rules weaken decision-making processes relying on them. This not only manifests the absence of essential regulations that the legislator should provide for with regard to compliance but leads to a weakening of supervision.

[34] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/tackling-discrimination/equality-bodies_en

Particularly problematic (because, at least under the laws of many Member States, no protection is afforded by anti-discrimination law) are cases of discrimination in which no specific person is discriminated against, but an entire group of people is disadvantaged (e.g. Tobler 2005; Ellis & Watson 2012). This can lead, for example, to certain job advertisements not being taken up at all by members of a specific group, or to its members having to pay a higher price for certain services. In the EU, Member States have an obligation to prevent discrimination, and to sanction violations of the provisions prohibiting discrimination, by applying effective, proportionate and dissuasive measures, regardless of whether any specific person is disadvantaged by the violation and can claim legal protection as an individual (CJEU Case C-54/07). Equally, however, problems also arise in cases where an effective remedy is not available exclusively at the individual level. In such cases, it must be shown that an apparently neutral rule, practice or decision disproportionately affects a protected group and is thus prima facie discriminatory (Zuiderveen Borgesius 2018). Effective protection against such discrimination would require, first, that it be recognised. The GDPR does not provide for an obligation to inform, especially in areas where AI is used only as an assistant (Sesing & Tschech, 2022).

Recently, some of these regulations have been translated into impact assessment tools to identify, assess and address adverse effects on rights, for example in the form of Data Protection Impact Assessments and Human Rights Impact Assessments. Besides helping companies to assess risks, these tools can require that a company or organisation modifies their products or procedures to improve their effects on data protection or human rights.[35]

2.2.2. Beyond legal efforts

The European Commission has also taken new directions in research on the use of digital technologies. Nearly 300 research projects dealing with different dimensions of democracy and its contemporary challenges, including digital technologies, received more than EUR 700 million under the Horizon 2020 research funding programme (2014-2020). The projects addressed a wide range of themes: democratic participation, trust and governance, the rule of law, Europeanisation, the challenges presented by harmful information, media literacy, civic education and global governance, the future of democracy, deliberative democracy, countering violent extremism and populism, transforming public services into citizen-centric and innovative services, and many more issues (EGE hearing of DG RTD.D4, 2022 on the European Commission's research and innovation funding for democracy and governance[36]). Horizon 2020 also funded experimentation with democratic innovations, in particular deliberative and participatory democracy approaches.[37]

[35] The Dutch government, for example, is increasingly making use of these to analyse and assess risks of using digital platforms, for example the use of Facebook pages. An example is: https://www.privacycompany.eu/blogpost-en/human-rights-impact-assessment-of-facebook-pages

[36] See also https://research-and-innovation.ec.europa.eu/research-area/social-sciences-and-humanities/research-and-innovation-funding-democracy-and-governance_en

[37] See this report on Horizon 2020 research on deliberative and participatory practices in the EU: https://op.europa.eu/s/yMM6

Horizon 2020 also supported, as part of the Green Deal, a participatory action on the green transition involving 800 citizens from all Member States and resulting in roadmaps for sustainable food systems, smart and efficient mobility, and energy-efficient buildings.[38]

In addition, research on democracy and governance is specifically funded under the Horizon Europe research funding programme (2021-2027). With a dedicated budget of EUR 264 million over its first four years, it is the most substantial allocation of resources yet for research topics pertaining to social sciences and humanities. Some of the challenges identified in this Opinion are also being addressed in funded projects. For example, some projects are specifically addressing the impact of AI and big data on democracy[39]; some are dedicated to understanding and countering foreign interference. Other research themes include the impact of inequalities on democracy, the future of democracy and civic participation and how they can be supported (or threatened) by digital technologies, how to improve the inclusiveness of public spaces online and offline, and the threats posed by disinformation, polarisation and extremist narratives on online media.

2.2.3. Technology for democracy and value-sensitive design

As noted, for democracies to become or remain strong, several conditions must be met: rule of law, transparency and accountability, participation, legitimacy of institutions, adequate and functioning regulatory and institutional mechanisms to protect fundamental rights and the ethical values they protect and promote, an economic system that is accountable to all people living in the society, and an independent judicial system – to name but a few of the more important ones. Whatever we value in our democratic and digital practices – equality of opportunity, fairness, tolerance and respect in the public sphere, or solidarity – these values need to be supported and facilitated by digital design. And vice versa, if we do not strengthen fundamental values in the fabric of our democratic societies, we cannot expect digital infrastructures, models and algorithms, platforms, social media and communication systems to miraculously – as if by an invisible digital hand – be aligned with these values.

In the last two decades, experiments in the digital mediation of democracy have been carried out across Europe. Examples range from crowdsourcing constitutions in Iceland to petitioning platforms in the UK, and from deliberative assemblies in Ireland, open government data in Estonia, online deliberation platforms for city planning in Barcelona, to G1000 citizen councils in Belgium and the Netherlands. Ideas about inclusion, participation, voice, deliberation and public debate have

[38] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/final-report-our-citizen-voices-eu-climate-transition-project-out-2023-05-03_en

[39] Some examples: ORBIS elaborates new participatory democracy models by employing AI- and Big Data-based technologies; KT4D creates models to foster more inclusive civic participation, with strong involvement of CSOs; ITHACA improves the understanding of how AI-based solutions can be used in the field of civic participation, in full respect of fundamental rights, and in light of moral and ethical reflections; AI4Gov develops evidence-based innovations and policies to improve public participation with the use of AI- and Big Data-based technologies, while complying with fundamental rights and values.

found expression in these and many other socio-technical experiments. It is in this spirit that the Conference on the Future of Europe was convened, in 2021-2022, involving notably an interactive digital platform and citizens' panels. Among its results was a series of proposals on how citizen participation and youth involvement may be strengthened at EU level.[40]

Such exercises and initiatives need to be supported and scaled up by the European Commission. Examples of this are the Citizens, Equality, Rights and Values (CERV) programme[41] and the Competence Centre on Participatory and Deliberative Democracy.[42] In fact, Naeem (2019: p. 41) points out that the benefits of open government[43] can include lower levels of corruption, higher levels of public awareness and education, higher level of transparency, more democratic control, and improved efficiency and effectiveness of public services.[44]

What applies to safety, privacy and security is true for other values as well: besides strengthening these values through policies shaping social, economic and political practices, we also need to realise them through design. 'Design for values' thus refers to the explicit transposition of ethical values into context-dependent design requirements. It provides a framework for stakeholders to translate moral consideration (e.g. those pertaining to fundamental rights) into context-dependent design requirements through a structured, inclusive, transparent process. The European Commission has been championing such an ethics-by-design approach (e.g. in the GDPR and the proposed AI Act), and now many are following Europe's lead. It is time for the EU to expand the ethics-by-design approach to democracy itself.

Digital (social) media have not only created echo chambers and filter bubbles,[45] and isolated, segregated and polarised our societies, but also led people astray and pitted them against each other in terms of 'likes' and 'followers'. If people no longer cherish democratic values, all our policies and best laid schemes will fall upon deaf ears. At the same time, with the right design, online platforms can support civic engagement and encourage inclusive discourse – if they are not, as is currently often the case, designed to hold the user's attention for as long as possible to generate advertising revenues. Initiatives in value-sensitive technology design have recently sprung up partly within university research projects, offering public alternatives to profit driven platforms.[46] In addition, legal and financial incentives

[40] See https://futureu.europa.eu/en/

[41] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/justice-and-consumers/justice-and-consumers-funding-tenders/funding-programmes/citizens-equality-rights-and-values-programme_en

[42] See https://knowledge4policy.ec.europa.eu/participatory-democracy/about_en

[43] Open Government refers to the idea that the actions of government should be transparent and accountable (e.g. Meijer et al 2012; OECD, Open Government).

[44] On the notion of openness, and that it should never be treated as an end in itself (see, e.g. Hartley et al. 2018; for the field of open science, see Leonelli 2023).

[45] A seeming paradox is that some studies suggest that being confronted with political opinions that differ from one's own can lower political interest and engagement (EPRS 2018), yet echo chambers are generally regarded as problematic.

[46] For example, PubHubs is a non-commercial community network developed by academics at Dutch universities, which offers an online environment made up of 'hubs' – or communities,

should be created encouraging for-profit companies to invest in measures that strengthen public deliberation and pluralistic dialogue even when these do not translate into commercial profit.

such as sports clubs, patient organisations, museums or municipalities – in which people can safely and securely communicate. The network focuses on reliable information, protected, if necessary, with digital signatures, and on trusted communication, if necessary with guarantees of the identity of participants. Importantly, it is not driven by a business model which requires collecting personal data. Such non-commercial alternatives should receive more support from national and/or supranational public bodies (see also, e.g. von Thadden 2023; Staab 2019).

3. NOVEL RISKS AND CHALLENGES TO DEMOCRACIES IN THE EU

3.1. The expansion of Big Tech into new sectors

Adding to the risks mentioned above (Section 2), we now identify a number of novel risks that digital technologies present to democracy, specifically to the richer, 'thick' conception of it.

In the past decade, vast technology companies such as Alibaba, Alphabet, Amazon, Apple, Baidu, Meta, Microsoft, Tencent and Xiaomi have come to dominate the world of computational hardware and software, and to manage most of our internet searches and social media.[47] In the process they have expanded well beyond their original spheres of activity into other areas and markets, including health and medical research, education, transport, news provision, public administration, agriculture, finance, law, humanitarian aid, and so on.[48] Drawing on the political philosopher Michael Walzer's (1983) theory of justice and complex notion of equality, we can understand this expansionism as a series of 'sphere transgressions' that pose novel risks to democracies (see also Sharon 2021a, 2021b; Van den Hoven 1997; Nagenborg 2009).

According to Walzer, society is made up of spheres of practice distinguished by a defining good or cluster of goods – e.g. the economic sphere, the sphere of politics, the sphere of welfare, family life, education, and so on. In liberal democracies, Walzer argues, we can accept some inequality within spheres: some people may be richer than others (successful entrepreneurs), some people may have more political power than others (political leaders) and some people may receive more healthcare (the chronically ill). But it is particularly problematic if these inequalities are carried over from one sphere to another. The fact that some people have more access to money and other resources than others should not entitle them to better healthcare or enable them to buy votes. Nor should the fact that someone has more political power than others mean that they receive better education for their children or privileged access to the market. Such translations of advantage between spheres disrupt complex equality and can lead to the domination of some members of society by others (Walzer 1983).

Big Tech corporations have gained an advantage in their original sphere of activity – because they are good at what they do, or they have had pockets deep enough to buy out potential competitors. As a result, they hold quasi monopolies in certain capabilities, such as the development of data collection, storage or analytical products and services. Through sphere transgressions, they convert their position in one sphere of activity into advantages in new spheres. These conversions can be

[47] Several seminal works have described this, including Zuboff's *The Age of Surveillance Capitalism* (2019) and Cohen's *Between Truth and Power* (2019).

[48] For an overview of tech corporation initiatives in various sectors see https://www.sphere-transgression-watch.org/.

seen as problematic encroachments into new spheres, insofar as these corporations do not have the domain expertise required by their new level of influence in new spheres such as health or education, and insofar as they are not accountable in the way that public sector actors are. Indeed, they function outside of the legal and normative checks and balances of democratic systems.

In the political economies in which digital practices are embedded, such sphere transgressions pose a number of risks to democracy. These include: (1) privacy harms, (2) non-equitable returns for the public sector in its collaborations with tech actors, (3) the reshaping of critical public sectors according to the interests and values of commercial entities (agenda-setting), and (4) deepening dependencies on Big Tech for the provision of basic goods or services.

3.1.1. Privacy harms related to sphere transgressions: The tip of the iceberg

As noted, many of the tech giants are notorious for their questionable privacy policies and data sharing practices *within* their original spheres of activity. Such privacy concerns may become even more serious when these companies move into new critical sectors and spheres, especially if particularly sensitive kinds of personal data, such as health and medical data, or data collected on children in schools, are in question. Privacy breaches in the new sectors into which technology companies are making inroads can be very consequential – for example, if they are used to help determine future decisions about which patient gets a certain treatment, which school a pupil can go to, or which parent receives a welfare benefit.

In one sector into which Big Tech companies are aggressively expanding, health, there have already been several incidents involving privacy breaches. In 2016, DeepMind, Google's AI offshoot in London, was at the centre of a data protection controversy when it was revealed that a data sharing partnership with three NHS hospitals allowed it to access identifiable health data on 1.6 million patients without their explicit consent (Powles & Hodson 2017, 2018). An investigation conducted by the UK's Information Commissioner's Office (ICO) ruled that the data agreement breached data protection law (ICO, 2017). Then, in 2019, Google came under scrutiny when its partnership with Ascension, the second largest health system in the United States, granted the company access to over 50 million medical records (Copeland 2019). Here too, the data was not anonymised, nor were patients or doctors notified, or asked to provide proper consent. More recently, in 2022, Meta has been criticised for accessing medical data on millions of people and using it for targeted advertising via a data tracking tool called Meta Pixel. The latter is installed on dozens of hospital websites in the US, granting the company access to data on patient appointments, prescriptions and health status (Delouya 2022).

European rules and regulations protecting personal data drafted over the past decade – from the GDPR to the DGA and the more recently proposed Data Act – aim to address this type of risk. They do so by reaching an appropriate balance between competing rights and interests, such as between data protection and data processing interests. In addition, privacy- and data-protection-by-design methods

(see Section 2.2.) can be developed and applied by tech actors in collaboration with public institutions.[49]

Privacy harms, however, are only the tip of the iceberg when it comes to the novel risks to democracy posed by Big Tech expansion into new sectors (Sharon 2022). This is because the business models that drive the expansionism are not primarily about selling personal data to third parties – be these advertisers, insurers, or anyone else. The latter is a business model that we know a fair bit about from its operation in internet search engines and social media, and for which regulatory instruments such as the GDPR and privacy-by-design techniques (Aizenberg & Van den Hoven 2020) are quite well-equipped. But where many initiatives in new sectors are concerned, the tech corporations are not collecting data to resell it, and revenue will not be generated through data collection and processing. For example, the ResearchKit software – one of Apple's most ambitious health initiatives that allows clinicians to carry out studies using the iPhone to collect health data – does not require data to flow to, or through, Apple. Instead, the business model rests on the software and the iPhone being used by more and more clinicians for decentralised and remote studies – a form of research which is on the rise.

Moreover, some technology companies effectively instrumentalise privacy as a means of extending their reach into new sectors. They take advantage of the heightened focus on privacy and data protection, in other words, to move into new sectors with privacy-friendly products and services. A good example of this is the application programming interface (API) for digital contact tracing that Apple and Google jointly developed at the outbreak of the COVID-19 pandemic. This was explicitly built in a way that would conform to stringent privacy-protecting criteria defined by leading European privacy experts, in particular, decentralised data storage (Troncoso et al. 2020; 2020/2616(RSP)). The protocol developed by Google and Apple complied with these criteria and was applauded by privacy experts and data protection bodies alike for its privacy-friendliness (Whittaker 2020). This API was subsequently adopted by numerous countries around the world – some of which redesigned the contact tracing apps they were already working on to comply with the criteria of the Google Apple API. In this way, the reach and influence of these companies into pandemic containment strategy and public health extended even further. Privacy-friendly technology can, therefore, unwittingly facilitate the increased involvement of tech corporations in the public sector. It is important that policy makers and regulators do not get "blind-sided by privacy" (Sharon 2021b), at the cost of ignoring structural issues relating to the distribution of power and agency in digital societies. They must remain vigilant to the broader risks that Big Tech expansionism in new sectors raises beyond mere privacy and data protection.

3.1.2. Non-equitable returns for the public sector

A rather different, and important, risk presented by Big Tech expansionism is that the public sector is not securing a fair share of the gains resulting from

[49] See e.g. the PEP framework (Verheul and Jacobs 2017), developed and implemented in a research collaboration between a university medical centre in the Netherlands and Verily, which uses polymorphic encryption and pseudonymisation to ensure data protection.

collaborations between the public sector and tech corporations (Mazzucato 2021; Bradley et al. 2022; Prainsack et al. 2022). This is particularly important in situations where data is being used primarily in the creation of commercial profit. One of the business models known to be driving Big Tech expansionism in new sectors involves access to domain-specific datasets. An example is medical data collected and collated in hospitals, which is needed to train machine learning to develop applications and algorithms. These algorithms are typically proprietary and can be monetised. Often, tech companies give collaborators in the public sector access to the algorithms at no cost. But this is typically for a pre-determined period, after which access comes with a steep price tag. In the DeepMind-NHS collaboration, for example, DeepMind was using patient data from several hospitals to develop an app to help professionals identify patients at risk of acute kidney disease. Initial contracts of five years meant the hospitals involved could use the app at no cost, but after that DeepMind was free to set a price for use and access. Other partnerships between British hospitals and DeepMind for different kinds of AI research followed the same pattern. The development of proprietary algorithms trained on publicly funded datasets can be likened to drug innovation, where pharmaceutical companies create patents developed through research carried out in part using public financing.

During the COVID-19 pandemic, which saw numerous collaborations between tech firms and public sector institutions for data analytics and other purposes, awareness of this risk increased. In the UK, for example, the NHS entered into agreements with Google, Amazon, Microsoft, Palantir and Faculty (a British AI start-up) in a project that sought to create a 'data store' collating data from across the NHS capable of providing a dashboard of information to support pandemic decision-making (Gould et al. 2020). A freedom of information request led by the civil society organisation Foxglove revealed that the companies were originally granted intellectual property rights and allowed to train their models and profit from access to NHS data, raising concerns not just about privacy, but about whether the public was getting "fair value for [their] NHS data assets" (Fitzgerald and Crider 2020). The terms of this deal were amended following this revelation.

This dynamic is present not just in the healthcare sector but all sectors in which underfinanced public institutions are lured into partnerships with tech companies via incentives of seemingly no-strings-attached private investment. Policymakers and sectoral actors need to become more alert to the fact that, in the long run, the public sector is losing out in these partnerships. To counter this, and to ensure more equitable allocation of value creation, more robust contracts with suitable terms and conditions need to be attached to these partnerships.

3.1.3. Agenda-setting for commercial interests

The more involved in public sectors tech corporations become, the greater their influence also on what research is carried out. When tech-affiliated philanthropists become major funders of disease research as well as research in other fields, a gradual reshaping of sectors in line with the values and interests of shareholders and top executives at tech corporations can occur (Prainsack 2020; McGoey 2015).

One example of this is Alphabet's now long-standing interest and investment in Parkinson's disease research, which includes the development of a 'wearable' for clinical and diagnostic research, investment in smart utensils for people with Parkinson's, and over US$1 billion in funding for Parkinson's research channelled through a philanthropic foundation set up by Sergey Brin, a co-founder of Google. Parkinson's is a currently incurable neurodegenerative disease afflicting some 10 million people worldwide which deserves the substantial attention it receives. But the investments in research into treatments for it associated with Alphabet are also rooted in Brin's personal interest in finding a cure for the disease, as he is the carrier of a gene linked to Parkinson's – something he has been publicly open about (Dolan 2022). Furthermore, while Brin's philanthropy is, in this case, of apparent value to global health, it is known that a number of founders and executives at tech corporations, including those at Amazon, Palantir and Alphabet are actively investing in areas which may be of reduced importance in terms of global health, such as life extension and anti-ageing (Gebru; Sample 2022).

In strong democratic societies, research agenda setting has to be the outcome of some form of public deliberation wherein the interests of all and the vulnerabilities of the weakest are taken into consideration. Moreover, public bodies must be able to audit the ensuing studies and ensure that the data and outputs are used for the public good. The influence of private actors and philanthropists with vested interests of their own on research priorities should remain limited.

3.1.4. Deepening dependencies on Big Tech

One of the greatest risks for democracy raised by the spectre of Big Tech expansionism is the deepening of existing dependencies, and the emergence of new ones, in which the public sector eventually becomes a 'junior partner' to private actors – in this case a handful of non-European private actors who are neither transparent nor accountable in the way expected of public sector actors, or indeed private contractors working in the public sector (Taylor 2021). An important avenue through which this can occur is through the growth of these firms' *infrastructural power*. Gürses and Dobbe (2020) distinguish between "common infrastructure" (i.e., the familiar traditional infrastructure of, for example, water, sewage, road and railway systems) and "computational infrastructure", which they define as the global network of data centres, network infrastructure, and mobile devices and platforms. The latter is becoming essential for the provision of digital services. Yet the components of the computational infrastructure are owned and run by the largest of the tech corporations: Microsoft (e.g. Microsoft 365), Amazon (Azure), Google and Apple (iOS). Also here, the problem created by a deepening of dependencies does not emerge only from the risk of data being misused. It arises from a growing dependency of the public sector on these infrastructures. The result is often the divestment of public funding and a decline of public expertise.

In their infrastructural role, the products and services offered by technology firms need to be seen as elements of a 'suite', or ecosystem, which cannot be bought into without taking on the whole series of hardware, software, apps, cloud and operating system, which individual products (inter)operate with. Threats to democratic and other values are not created by digital technologies as such. They come from the ways in which technologies are used, what they replace, and whether they make

powerful actors even more powerful while disempowering others. Gürses and Dobbe (2020) speak of a deployment of computational infrastructures onto common infrastructures in this context. While our public infrastructures have not yet been completely digitised or subsumed by computational infrastructure, we do increasingly rely on computational infrastructures for the proper functioning of important areas of society. That is, our public infrastructures are increasingly becoming computational infrastructures (think of electronic health care records or digital banking systems). This development can lead to a dangerous dependence of public sectors on Big Tech firms in carrying out their main task, the provision of public services and goods, and to the undermining of the "publicness" of public sectors (STOA 2022[50]).

The digital contact tracing API referred to above illustrates just how entangled and dependent our daily lives have become with, and on, computational infrastructures, and how this can affect a sector such as public health. Google and Apple's almost complete monopoly of smartphone operating systems meant that the very attempt to automate contact tracing with smartphone applications put public health authorities and governments at their mercy (Veale 2020). If interoperability is sought – as was the case with contact-tracing apps – it would make little sense to develop apps that cannot run on Google or Apple's operating systems.

Another example is the extent to which education has become increasingly dependent on digital platforms and infrastructure, especially during the pandemic and the rise of remote lectures and lessons (Fiebig et al., 2021; Kerssens and van Dijck, 2021, 2022). While the depth of these dependencies varies from country to country, and from institution to institution, the authors of the papers just cited point out that one of the main issues created by the migration of universities to public clouds, and the use of edtech in primary and secondary schools, is autonomy: be that in the form of academic independence or the institutional pedagogical autonomy of schools.

Public health and education are two of the basic goods that democratic societies should provide. Increased dependence on private actors in the provision of these goods – actors who are not regulated in the same way that public actors are, are not held accountable for serving the public interest in the way that public actors are. Neither are they subject to public scrutiny in ways that enable redress – is a threat to democracy that requires urgent attention in European policy making and regulation.

All of these risks raised by Big Tech expansionism point to the need for broader issues, and specifically the public-private trade-offs, to be taken into account when the public sector considers collaborating with tech corporations. Indeed, while there is much value to reap from these collaborations given the technical capabilities the tech sector has to offer, the risks, including the gradual reshaping of public sectors and the entrenchment of new dependencies, are neither immediate nor straightforward. We need to develop policy and regulation that captures this broader societal view and takes into account the longer-term future so that all people in

50 https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf

Europe can benefit from the collaborations in ways that protect the primacy of democracy.

3.2. Regulatory gaps, unintended overlaps, and contradictions in new laws

As noted in Section 2, the European Commission has been very busy over the past few years developing new legislation to address potential digital harms and improving its governance of digital innovation. In the process it has sought, in various ways, to mitigate the risks posed by the increased digitisation of society and to ensure that digital transformations take place in line with fundamental rights and values in Europe – and indeed to strengthen our democracies. Existing regulations primarily affect *vertical* relations between state actors and citizens. However, they also affect private actors' obligations to citizens in digital policy, and they complement one another, aiming at providing comprehensive protection. The regulations impose several implementation obligations on EU institutions as well as Member State administrations: for example, to create accountable administrative bodies and infrastructures, to assign new tasks to existing bodies and institutions, and to put in place measures that implement, operationalise and enforce data subjects' rights. However, several regulatory gaps and unintended overlaps, duplications and contradictions between the provisions laid down in legal instruments have been identified and still need to be solved (e.g. Bertuzzi 2023).

When it comes to the type of regulation required to address the scope and modalities of digital technologies on the basis of values and ethical principles, it is often difficult for legislators to define substantive rules from scratch. This can be the case, for example, when the ethical and societal evaluation of the technology in question is still pending. For example, the DSA tries to hold commercial actors such as large online platforms to account by, among other things, mandating stricter rules on the removal of illegal content (Regulation (EU) 2022/2065: Art. 16 et seq.). Concretisation of what is to be considered problematic content is, as the term "illegal content" suggests, limited to an assessment of compliance with EU and Member State law. The restriction of the regulation to *illegal* content, however, is too narrow. Other types of harmful information, such as 'simply' false news and conspiracy narratives, can be just as harmful, but often they do not fall under the umbrella of illegal content. A further hindrance here is the possibility that neither service providers nor public authorities can generate, or acquire, the necessary knowledge to assess and evaluate the relevant risks within a short period of time.

Two important regulatory principles in this respect are the *risk principle*, which requires scientific evidence of the potential risks of a technology and adjusts regulation accordingly, and the *precautionary principle*, which allows the use of a technology that threatens to cause serious and irreversible harm to humans and/or the environment to be restricted even in the absence of reliable scientific evidence. However, these principles do not provide specific guidance clarifying, for example, the necessary trade-offs between competing interest positions condensed into legal positions. The various ways in which the principles are applied, together with the paucity of case law illustrating their regulatory implementation, also make their uniform and context-specific application difficult where trade-offs are concerned.

The actions of public administration often involve factual investigation of whether an intervention is necessary and then consideration of what legal measures, if any, are required. This two-stage examination is in many cases characterised by a margin of judgement at the factual level and a margin of discretion at the legal consequence level. However, if the legislature, which must regulate a large number of different practical scenarios, lacks the knowledge necessary for determining exactly what decisions the administration should make in the relevant context, administrators are required to 'close' the legal knowledge gaps, and to determine the legal consequences. With the increasing freedom being given to administrative bodies, there is the risk that the application of the law will depart from the intentions of the legislature or fail to be as consistent as it should be, leading to variability in the preservation and implementation of values. This situation is further complicated when administrators themselves lack expertise in the digital domain. That puts them at a disadvantage vis-à-vis private actors, who have extensive technological knowledge and expertise. It also limits the administration's ability to monitor and exercise oversight.

It is also true that, at present, we have an insufficient number of measures in place that put the digital expertise of private actors at the service of public interest (and sometimes even public administration) – for example in the form of public private partnerships (PPPs) that involve contractually regulated cooperation between a public body and a private company within the framework of a special purpose vehicle. In many cases, PPPs introduce a division of labour in which the private partner takes responsibility for the efficient delivery of services, while the public body ensures that the objectives, defined by public interest, are achieved, and that the necessary funding is provided. Sometimes, PPPs are motivated by problematic assumptions, such as the belief that privately owned social media platforms are unique sites of pluralism and participation, or the opinion that technologies can only advance thanks to private sector investments, and the public sector must take what it is given. Moreover, PPPs can be detrimental to democracy if they contribute to further sphere transgressions (see Section 3.1.), and to a greater withdrawal of public actors from technology development. Another problem is the excessive influence of tech corporations on the exercise of fundamental rights, such as freedom of speech and the right to information.

In addition to regulatory gaps at the legislative level and knowledge gaps in public administration, nuanced specific provisions within different legal instruments can contribute to fragmentation. This happens, for example, when different legal instruments apply to similar, or even identical, contexts and facts. Fragmentation, in turn, can undermine the very objectives that regulatory measures were designed to achieve – for example the protection of fundamental rights. They can create confusion among those who apply the law, since neither the bearers of the obligations nor those to whom those obligations are owed know what rights and obligations the legal framework defines.

As an illustration of these issues, we can take the rules on data processing. These are broadly scattered across a multitude of new and recent EU legal instruments on digitalisation. In their substantive scope, the rules overlap – for example in terms of the data, the parties (including data processors), and the technologies to which they apply.

A more specific example, at EU level, is the following. The parallel, simultaneous application of the GDPR, the AI Act and the DGA would oblige companies to take on

different roles: under data protection law, as 'controllers', 'joint controllers' with other entities, or 'processors'; a 'data holder' role under the DGA; and a 'developer' role under the AI Regulation. These roles are not harmonised in a coherent and clear assignment of bundled obligations of the kind that would be vital for the addressees of the relevant laws and associated monitoring and oversight bodies. As a result, the actors who are assigned the duties by law are regularly unclear about what duties, exactly, are being assigned to them, and in which role. Overlapping or conflicting allocations of duty remain unresolved at the regulatory level and are not addressed through appropriate governance measures. Other specific examples of laws in conflict include the duplication of protective measures (e.g. applying data protection rules to anonymised data based on a vague definition of when data is legally considered anonymised) and the inappropriate shifts in the trade-offs between conflicting interests that result from this. They also include the dissolution of safeguards by rules that effectively cancel each other out – e.g. when the same actors have conflicting obligations to fulfil.

The monitoring and enforcement of conflicting and non-harmonised regulations is often ineffective because it is exercised by different bodies. The regulatory discordance leads to scattered audit and oversight structures to be created, resulting in a patchwork of competencies among different bodies, and in overcomplicated administrative oversight and enforcement structures overall. Additionally, even when the obligations are clearly defined – as is the case, for very large online platforms, for example, in the DSA – they follow principles of private law enforcement and self-responsibility by the service providers. For example, they leave it up to the provider to decide on the legality of the content it hosts and its removal or its blocking. Even where official orders against illegal content are available under EU or national law, in enforcing and complying with applicable law, providers are primarily encouraged to self-regulate – for example by adapting General Terms and Conditions, and defining community standards, content moderation, risk mitigation, or codes of conduct. It remains to be seen whether, and to what extent, providers will be willing to comply with these self-regulatory obligations and adapt their systems accordingly. The proposed countermeasures – fully implemented – would in some cases seriously shake up the providers' business models (Kuhlmann & Trute 2022). It is also questionable whether the supervisory authorities and courts can prosecute violations of the applicable law effectively given the sheer volume of new content.

The fragmentation of specific regulations in the digital domain can be observed not only between EU secondary law measures, but also within individual secondary law instruments. It also arises at different regulatory levels – for example between international law and EU law, EU law and the law of third countries, and EU law and the law of the Member States. Where the interaction between EU law and Member State law is concerned, the main challenge is the mutual influence of sectoral regulations. The various impacts that the regulation of one sector or area has, often unintentionally, on other sectors and areas, particularly on the enforcement of their rules, can lead to an undesirable fragmentation of laws with the same, or similar, substantive scope. For example, many non-EU social media companies are registered in EU countries to benefit from low tax rates. The fact that the responsibility for data protection monitoring and oversight is generally assigned to the supervisory authorities of the countries in which the companies are registered, and that they are often not well equipped to handle a large number of complaints in a timely manner, has created a bottleneck in the handling of data protection

complaints by these authorities in connection with international data transfers. This bottleneck has recently been resolved by the Court of Justice of the EU (CJEU Case C-645/19). The Court has extended the responsibilities of the data protection supervisory authorities of Member States, clarifying their mutual obligations to exchange information and creating new possibilities for filing complaints in connection with the consistency and cooperation procedure between supervisory authorities set out in the GDPR.[51]

While it is true that interaction between EU law and national law related to various legal regimes and sectors must fit into the complex system of division of the competences between Member States and the EU, the interpretation of EU law by the CJEU could nevertheless benefit from this interaction. However, the introduction of such interpretation through case law is only possible if relevant facts are presented to the courts, and the ensuing proceedings take a long time.

The objective of the GDPR is to ensure both the protection of data subjects' rights and the free movement of data. In determining the proportionate balance of these objectives, risks to the rights and freedoms of natural persons that may be affected by a particular data processing operation must be taken into account, with consideration being given to all of the affected fundamental rights and freedoms under CFREU as well as rights guaranteed by secondary legislation. The principle of proportionality also applies to international data transfers. Since the level of protection provided for in EU law must 'travel' with the data wherever it goes, conflicts between the GDPR and third country data protection rules are bound to arise in cases where both can be applied if third country data protection rules differ from those of the GDPR, and there are no mechanisms to resolve such a situation.

At the same time, new legislative proposals appear to double down on data protection by, for example, treating access to personal and sensitive data in a secure data space as an international data transfer when actors outside the EU/EEA request access. Access to data in an EU infrastructure follows technical specifications that comply with the standards of EU data protection law. If data cannot leave the secure data system and can only be processed within the infrastructure according to EU standards, no further, and different, obligations should be imposed on European and international actors as users of the data, i.e., stricter access conditions should not be defined for international actors.

To protect the rights of data subjects and to comply with the principles of data minimisation and purpose limitation, sensitive data is usually made available in anonymised form for secondary use, for example for scientific research. This is the case for electronic health data in the European Health Data Space (EHDS), to the extent that the anonymised data is sufficient to achieve the processing purpose of the data user. At the same time, data processing by users is limited to the technical infrastructure of the EHDS and does not allow users to download or otherwise reproduce the data in question. However, making data available in anonymised form

[51] The CJEU clarifies the powers of national supervisory authorities under the GDPR in that it empowers a supervisory authority of a Member State, under certain conditions, to exercise its power to bring an alleged breach of the GDPR before a court of that state. The supervisory authority can initiate or conduct judicial proceedings in relation to cross-border data processing, even if that authority is not the lead supervisory authority in relation to that processing.

would exclude their processing from the scope of the GDPR, so no further safeguards may be needed to maintain protection if the nature of the processing does not remove anonymisation. On the other hand, if safeguards are put in place, processing data in a non-anonymous format could still comply with applicable data protection rules. In addition, processing data in a non-anonymised format would avoid losing the analytical value of the data for research (Molnár-Gábor et al. 2022). By mandating anonymised processing as the main rule in an otherwise secure technical infrastructure such as the EHDS, the safeguards for data processing seem to be 'duplicated' and no longer reflect the proportionality that should be established between the interests of the processor and the interests of data protection. This proportionality or balance must also consider the data subjects' interest in the data processing, as well as the societal perspective that the data is being processed to ensure that public benefits are derived from the research results. In other words: By mandating protection within a data space designed according to applicable data protection standards and making anonymisation the main rule, the principle of proportionality seems to be disregarded.

4. WHAT SHOULD BE DONE TO PROTECT AND STRENGTHEN DEMOCRACIES IN THE EU?

As argued in this Opinion, strengthening democracy – as the form of government best suited to realise fundamental rights and core values of the EU such as justice, equality and solidarity – is an ethical necessity. Digital technologies can support democratic processes and structures in many ways: they can, for instance, facilitate voting and participation,[52] or foster access to information, education and healthcare. At the same time, there are substantial grounds for concerns regarding novel harms to democracy in the digital era. The opportunity to rapidly[53] spread false or manipulative information can have detrimental effects on public debate and democratic elections, and it can increase polarisation in societies (European Parliament 2021a). Privacy harms and ubiquitous surveillance can lead to pernicious uses of personal data and a contraction of the 'breathing room' that people need to act as autonomous, critical individuals (Cohen 2013: p. 1906). Other problems include the potential for new forms of discrimination resulting from algorithmic decision-making, non-equitable returns for the public sector from the commercial profits of digital businesses, agenda setting by commercial entities, and deepening dependencies on private technology corporations for the provision of basic public goods. All these developments threaten the values that a democratic system aims to protect.

Safeguarding values and fundamental rights cannot be achieved by governments alone: it requires the active participation of all people. However, it cannot be assumed that all are similarly interested in engaging or enabled to engage. In the following section, we outline the preconditions for active citizenship and democratic participation in the digital era. We call for efforts to promote people's digital literacy (including its technological and legal aspects, and critical thinking skills) and we argue for the need for an ethical framework governing interventions aimed at reducing harmful information and other problematic developments in the digital space. Finally, we address the importance of publicly funded research and of focussing on regulatory gaps.

4.1. Citizenship[54] in digital democracies

As noted, democracy – and in turn, citizenship – means more than mere participation in elections. The kind of citizenship that corresponds with the 'thick'

[52] Some expect that digital practices will change the nature of political representation in profound ways; digital technologies also provide opportunities for more forms of direct democracy – see, e.g. European Parliamentary Research Service (2020).

[53] Research found that false stories spread faster, farther and deeper than other types of information; see JRC 2019.

[54] Also here, we emphasise that our use of the term citizenship is broader than merely formal legal citizenship. It denotes people's roles and identities in the political communities they are part of.

conception of democracy that we promote in this Opinion requires people living in the EU to be willing, and to be given opportunities, to participate in political, social and economic life.

Participation of this kind requires several things. It requires that people trust the EU and its institutions, and that they are willing to engage actively in public life, based on a shared vision, and that they are confident that such engagement can have an impact. At least three preconditions can support this. First, transparent, fair and consistent policies and governance by EU institutions are a requirement for trust. Here, digital technologies and interfaces can be helpful in creating access to information and documentation that shows how and why decisions were reached – for example also by clarifying the values upon which decisions are based.

A second precondition concerns peoples' conception of themselves as political actors, and indeed as sovereign, rather than as mere private individuals and consumers. While democratic values do not necessarily clash with market logic, the latter hollow out the former when they take over all spheres of society (Soron & Laxer 2012). When people's wealth determines their access to healthcare and housing, and what schools their children attend, this increases inequalities and limits the spaces in which people from all walks of life and all social strata come together. Democracies require deliberation and other exchanges to take place in these spaces, and the commercialisation of public space limits these vital exchanges (Sandel 2020). The overarching power of market logic also explains why the EU's imperative to harmonise markets (here: digital markets) is often in tension with fundamental values such as justice, equality and solidarity. When markets become the reference point for all other values, 'fairness' is reduced to 'fair competition' and 'domination' comes to mean 'market domination'. In the focus on markets, moreover, individuals are reconfigured as consumers only, and companies are mere market competitors. Strengthening democracies in the digital era, by contrast, requires understanding fairness in its broad sense, involving equality and justice in and across all domains, not just the economic sphere, and ensuring that people's basic needs do not have to be met on market terms. Public services should insulate key values and needs – education, healthcare, housing – from market rationales and dynamics. And, more broadly, issues pertaining to the economy need to be included in the range of issues that people have a say in (see also Warren 1992). The notion of economic democracy (Sen 2009) emphasises that citizens also need to have agency over economic issues. The organisation of economies shapes how people work and live, what they learn in school, how much they earn, and many other things. It is too important to be left solely 'to the experts' or 'to the market'.

Third, encouraging democratic participation also requires providing opportunities and an infrastructure that allows citizens to engage with EU policies and institutions. The European Commission's "Have your say" platform[55] and the digital platform used for the Conference on the Future of Europe are good starting points for this. Again, digital technologies provide a range of means to facilitate these processes – for example through civic engagement platforms, e-voting or other e-democracy applications – nurturing a culture in which participation is perceived as an integral

[55] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives_en

part of everyday life and is facilitated (CDDG 2021; European Digital Competence Framework for Citizens[56]).[57]

4.2. Public education

In digital societies, the ability of people to participate in different aspects of political, social and economic life also depends on their digital skills, digital literacy and related abilities. These capacities are needed if people are to be able to manoeuvre through digital interfaces, be it simply to access information, to cast a vote, or to engage in a deliberative process. A more demanding aspect of digital literacy concerns the confusing intermingling of reliable and harmful information in the digital sphere. AI-generated content that is indistinguishable from human-generated content, often based on undeclared sources (Spitale et al. 2023), and the algorithmic creation of echo chambers, make it even harder for people to critically, and fruitfully, assess and use the information that is digitally available to them. Beyond technical and epistemic issues, citizens need to be informed about the potential benefits and harms of information sources, communication channels and engagement platforms in the digital space so that they can make informed decisions about whom to trust and which services to use. As not everyone is equally prepared or enabled to participate in public discourse, interventions fostering critical thinking, moral reasoning and effective and constructive communication can facilitate the participation of all social groups, together with interventions that foster the appreciation of public engagement itself. Legal literacy training can help citizens to harness the benefits and to challenge the negative power of digital technologies in the EU.

Interventions, for example training courses, of such kind can help us, as a society, to overcome digital divides, ensuring that everyone has the tools and capabilities to use digital technologies to participate fully in society, and that no one is left behind (e.g. the EU's Digital Education Action Plan[58], or Mimikama, an Austrian fact-checking site[59]). In a time when (often inexpensive) mobile devices have become the primary means of online access for many people around the world, digital divides go beyond the separation between users and non-users of digital technologies (see Prainsack 2017: p. 36). One divide is between those who use the internet mostly in a passive and basic way, and those who have the skills and means to use it in more creative and deeper ways – although the former may spend just as many, or even more hours online (e.g. Wei 2012; van Deursen and van Dijk 2014; Robinson et al. 2015). Lack of access is not the only reason for internet non-use. Some people choose to remain offline due to what media and technology expert David Brake calls "motivational" access barriers (Brake 2014), referring to people who feel that the internet does not have anything worthwhile to offer, or who are concerned about privacy (see also Morrison & Gomez 2014). Alternative access

[56] https://ec.europa.eu/social/BlobServlet?docId=15688&langId=en

[57] In a non-paper, the EU Digital Citizenship Working Group set out, in 2022, five pillars of digital citizenship, recommending policy actions in areas including technology, social engagement, human rights and democratic participation (Killeen 2022).

[58] https://education.ec.europa.eu/focus-topics/digital-education/action-plan

[59] https://www.mimikama.org/

to services, in particular in healthcare, must be guaranteed to people who prefer not to enter the digital sphere.

4.3. Ethics frameworks for interventions to counter infodemics

Those using digital interfaces need to be able to recognise reliable information. They require tools that enable them to autonomously judge and critically evaluate the quality of the information they receive.[60] On the other hand, information provided by public authorities including the EU institutions must be inclusive as well as tailored to the intended user groups, notably to those who are not 'digital natives'. Tools that encourage users to participate in digital initiatives can offer new opportunities for sharing knowledge and information, especially when these are aimed at groups who are at risk of marginalisation in digital societies, such as the elderly. Such tools could also help to broaden public debates that are otherwise restricted to the digitally literate or other elite groups.

The task of judging the quality of information cannot, however, be left to individual people alone. This is why, in response to fake news and other manipulative strategies that threaten democracies today, institutions are increasingly considering the use of social listening, social marketing and even social engineering strategies. See for example the work of the WHO on "an ethical framework and tools for social listening and infodemic management".[61]

Toxic content – including racist, sexist, homophobic, xenophobic and otherwise hateful forms of speech – circulating widely on the internet is now also reproduced by chat bots. One means of addressing this is content moderation, but it is by no means a silver bullet. First, because the contextual nature of language makes automating this task extremely difficult, if not too dangerous or even impossible.[62] Second, because content moderation – certainly in the form of the monitoring of hateful speech and horrendous images – is arduous, tedious and traumatising work for humans to carry out. Most tech corporations outsource this "ghost work" (Gray & Sury 2019). The result is that precarious workers in Africa and Southeast Asia, working in problematic conditions, are responsible for this task, thereby exacerbating unequal labour relations between the Global North and the Global South. These difficulties will only grow with the integration of large language

[60] The ERC project BOTFIND developed a 'junk news aggregator', a publicly available set of tools to evaluate news quality online. Similarly, the ERC project FARE AUDIT is currently designing a tool to audit search engines with the aim to detect disinformation in real time (these and the other European Research Council projects referenced here were brought to the attention of the EGE by the Feedback to Policy team of the ERC Executive Agency). At the EGE's public round table on Democracy in the Digital Age, reference was made to GPTZero, a platform developed in response to ChatGPT, that can be used to detect AI-generated content.

[61] https://www.who.int/news/item/10-02-2023-who-kicks-off-deliberations-on-ethical-framework-and-tools-for-social-listening-and-infodemic-management

[62] Yet, there have been many attempts to develop automated solutions, for example in the context of the ERC project AI4Dignity.

models, such as ChatGPT and Bard, into search engines and their widespread use by citizens.

Going far beyond matters of content moderation, AI-based predictive analytics can be used to nudge and affect the behaviour of internet users in a targeted way. Such strategies may lead to a 'digital arms race' to influence public opinion rather than to participatory democratic discourse. Understanding knowledge gaps, emotional reactions and behavioural dispositions can be used for providing targeted information to people (Spitale et al. 2021). The Cambridge Analytica and Team Jorge scandals provide shocking examples of this[63] and solutions must be found for ensuring that those employing these services (political parties, individual politicians, or other actors), and those providing them can be held accountable.

The points above lead to one last crucial consideration. Particularly when important societal goods such as public health are at stake, there is a risk that core features of democracy will be undermined by well-intended but problematic efforts to silence dissenting and potentially harmful voices.[64] Action might be warranted in circumstances where a crisis threatens, but it would need to be guided by an ethics framework based on the principles of openness, transparency, inclusivity, intelligibility and privacy, that help to shape the key elements of risk and crisis communication (evidence, initiator, channel, publics, message and feedback) (Spitale et al. 2022). It is also important to ensure that urgent decisions made in a crisis do not flout democratic legitimation and that they remain open to public scrutiny (EGE 2022).

4.4. Publicly funded research and its results

An important concern which became especially apparent during the COVID-19 pandemic, relates to publicly funded research and its results. On the one hand, the EU has invested millions of euros in research carried out at public and private institutions and corporations. On the other, the private sector remains the only point of reference when it comes to the use of digital technologies, such as AI, in the public sector. When governments and public administrations seek to use technological applications to deliver public services, they tend to turn to private companies rather than publicly accountable institutions, such as universities (see also Larkin 2013).[65] However, privately owned companies often treat data and

[63] See e.g. The Guardian's continuous reporting on this, https://www.theguardian.com/world/series/disinfo-black-ops

[64] E.g. as discussed at the EUI's conference on Surveillance, Democracy, and the Rule of Law, https://www.eui.eu/events?id=544559

[65] Hecht (2009: p. 15) uses the term "technopolitics" to refer to the "strategic practice of [...] using technology to constitute, embody, or enact political goals". Törnberg (2023: p. 9) sees the attempt to "compete with - and even supplant - the regulatory role of public institutions" as a characteristic of platform capitalism, and argues that the owners of large digital platforms pursue the strategy to "unnest their proprietary markets from the larger public market of which it is part, making participants subject only to the taxation and governance imposed by the platforms themselves" (Törnberg 2023: p. 6). See also York (2022).

research findings as proprietary instead of developing prototypes and models that are made available to the rest of society.

This means that there is a strong misalignment between research funding and knowledge that leads to tangible benefits for the public: the openness of research, data, and science is obviously not enough to ensure that society benefits from the studies paid for with its taxes. It is necessary to ensure that innovation funded with public money in the EU remains in the public sphere. The development of AI-based translation software that includes minority languages is not a minor example.

4.5. Regulation: What steps to take?

4.5.1. Knowledge generation

Beyond supporting science through projects and policy programmes such as Horizon Europe, the EU should ensure that findings from scientific research are transformed into actionable knowledge for society, including for policy making. EU and Member State authorities should be able to draw on extensive empirical knowledge within the scope of their discretionary powers when implementing EU law principles and applying indeterminate legal concepts such as public interest. To this end, EU agencies could further streamline information gathering and provide assistance to prevent the spread of false and other forms of harmful information. This applies in particular to risk information.

4.5.2. Public private partnerships (PPPs)

Possible forms of cooperation between the public sector and private companies and the role played by the EU in establishing PPPs require more regulatory attention, especially as regards the design of such relationships in line with the CFREU. This could help to counteract the potential issues listed in Section 3, which include the crowding out of public expertise and control by the increasing expansion of power of large tech corporations. Conditions that could be written into PPPs might include, for example, an insistence on open-source software or the implementation of Human Rights Impact Assessments prior to a PPP being agreed on.

For PPPs to serve innovation and to strengthen democratic and other values at the same time, access to data needs to prevent a 'Matthew effect', in which powerful corporations benefit disproportionately compared to smaller and medium sized enterprises and public actors. Moreover, the commercial benefits from any data use should be shared with the public sphere (Prainsack et al. 2022).

Fundamental rights do not only apply to the relationship between individuals and the state, but they also influence the legal relationships between individuals, and generally between private actors. Committing private actors to the protection of fundamental rights is and remains of key importance. In addition to the horizontal force of fundamental rights, which generally affects relations between individuals and private actors, PPPs can directly bind private actors to the obligation to respect fundamental rights when they must act in the performance of a public duty. In all

PPPs, it should be carefully considered whether the private companies involved pose a risk to democratic and other values (e.g. via partnerships with other companies in autocratic countries, or via ownership or influence by non-democratic governments).

4.5.3. Technology as a means of fostering fundamental rights protection

Technological measures can help to minimise risks to the rights and freedoms of individuals. They can do so by helping to define the context of data processing that takes place. Technical design, such as secure data infrastructures, can also contribute to the implementation of the principle of proportionality and can help to ensure the protection of the rights and freedoms of data subjects.

In addition, the creation of a favourable technical framework for digitisation can serve as a basis for using data in the public interest while complying with clearly defined legal requirements. The technical environment will, in this way, become part of the governance.

4.5.4. Cooperation and enforcement

The rules in data-related legal acts must be coherent and consistent to be applicable. Given the current inconsistencies, there is a great need to guide implementation towards actionability of the new legal frameworks in compliance with the principle of subsidiarity in the EU, and to avoid regulatory gaps, also influencing effective enforcement. Where regulations already provide for the possibility of further specifying EU rules on particular topics in compliance with EU competences, this should be pursued (e.g. tertiary legal acts, e.g. Art. 40 GDPR codes of conduct for sectoral data processing).

In addition, different legal regimes can be mutually reinforcing in implementation and enforcement. An example of this are measures developed under antitrust law that can prevent the concentration of power related to data collection, culmination and aggregation, alongside data protection regulations and consumer protection.

4.5.5. The EU as an international actor

In the international field, protection obligations could also be implemented through technical solutions that are a translation of legal trade-offs and values, especially when not only individual data and information but information systems and infrastructures are affected on a cross-border level. In addition, the shifting of the protection of fundamental values to operators of networks and platforms needs to be accompanied by appropriate regulatory measures on EU and international level instead of leaving the development, implementation and monitoring of rules to the self-regulatory efforts of private actors (see criticisms of the DSA in Section 3.2.).

While strengthening human rights protections regarding transnational information flows is helpful in combating the effects of foreign interference on privacy, the EU could also play a more important role in unifying the rules that define these protections across countries in instances of different regulatory systems applying different data protection and privacy rules.

In this context, rules for solving conflicting data processing provisions between the EU and third countries with different constitutional traditions could more vigorously prescribe data processing rules in business-to-business (B2B) and business-to-government (B2G) contexts. For future specific rules on an international level, the Council of Europe's amended treaty on data protection law[66] could be a good starting point.

[66] Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

RECOMMENDATIONS

Since the end of World War II, Europe, European countries and peoples, as well as the nascent European institutions, have been at the forefront of democratic development. But democracy is a living and breathing ideal that must continually be strived for, that must be nurtured and defended. It is not just a political regime, upheld by elections. It is also a set of fundamental values, including respect for human rights and ethical values such as justice, solidarity and freedom. These values shape human behaviour and form the foundation of societies. Such an understanding of democracy implies a civic consciousness of engagement and the recognition of the importance of social, political and economic equality in society. Recent years have seen profound challenges to democracy understood not only as a political regime, but also to democracy understood in this 'thick' sense. Democracy is in peril.

Without being its sole cause, digital technologies have played an important role in this development. They have, in various ways, contributed to the spread of mis-, dis- and other problematic information, manipulation, polarisation and discrimination. Via the expansion of powerful technology corporations, digital practices have facilitated the spread of market logics into public sectors which are responsible for providing basic goods such as well-functioning democratic institutions, health and education to all. However, when the important set of values that underpin democracies are considered in their design and regulation, digital technologies can also contribute to safeguarding and furthering democracy.

To protect and to foster democracy, the European Union should adopt purposeful policies – which ought to be pursued by:

1. Thinking of democracy differently – A wider understanding of democracy

Democracy is, too often, problematically reduced to elections alongside very limited mechanisms that enable civic participation and the rule of law – without substantively accounting for the rule of the people and the protection of their interests. Democratic values and principles, such as equality, freedom, participation and accountability, mean little unless they are specifically and concretely enacted through democratic practices and institutions.

The EGE calls for a wider understanding of democracy as the evolving form of organisation that is underpinned by – and best suited to protect – shared values and fundamental rights, and that is driven by the search for – and best suited to attain – the continuing realisation of the common good. Such a conception of democracy also entails a civic consciousness of engagement and the recognition of the importance of social, political and economic equality in society. It requires civic solidarity and reciprocity that support just outcomes. It is, indeed, to be seen not only as a political system, but as a wider social system that also protects its own societal preconditions, including health care, education and housing for all.

The EGE calls upon all to strive towards and make real such a democracy; it calls upon civil society to demand it and make use of all democratic means and institutions in that regard; it calls upon those in positions of power to nurture and expand such institutions; and it calls upon all those who hold claims to expertise to explore how this can be furthered. What democracy means and how it works has to be continuously developed, and this very (democratic) process of becoming and envisioning needs to be safeguarded.

2. A more inclusive democracy

2.1. Public participation, civic education and critical digital literacy must be promoted and supported

Member States, EU institutions, and other public authorities need to provide digital education to all people in Europe in order to ensure digital democratic participation and engagement, enhancing access to information and strengthening public deliberation and pluralistic dialogue. Skills required for participating in public discourse should be purposely fostered in education, such as critical thinking, ethical reasoning and effective communication. Literacy training (in terms of digital, ethical and legal literacy) will help us all to both harness the benefits and challenge the negative power of digital technologies in the EU. In addition, public investment should foster the creation of platforms and other digital media, in some cases publicly owned, that support a public sphere that does not feed on polarisation and the spread of harmful information, but that instead facilitates participation, deliberation and dialogue. In this context, appropriate measures must be taken to ensure that digital divides are bridged, not only in terms of access to infrastructure and digital technologies, but also in terms of how people can use digital technologies and make their voice heard.

2.2. Digital citizenship requires social inclusion

Digital citizenship, understood as the ability to use (engage with and steer clear of) digital technologies in critical, collaborative and creative ways, also requires that people are able to recognise reliable information, having the tools that enable them to autonomously judge and critically evaluate the quality of the information they receive. It further requires that such tools be attuned also to groups who are at risk of marginalisation in digital societies, such as the elderly, disabled persons and persons living in poverty, and that research on inclusive digital technologies be encouraged.

2.3. More coherent regulation is needed to make digital practices serve people and communities

Digital technologies need to be regulated in such a way that they serve people and communities, instead of merely benefitting a small elite at the cost of most others,

becoming more transparent and accountable. The European Commission has taken an active interest in digital transformation, drafting legislation in response to this rapidly changing field, aiming to improve fundamental rights protection. But more must be done to address the risks that digital technologies create such as new forms of discrimination resulting from the use of algorithmic decision-making. Standardisation and alignment of regulation across the European Union to foster coherence and consistency needs to be further supported, also through mid-level sectoral rules, such as Codes of Conduct, by strengthening knowledge generation and by promoting technological solutions such as shared data spaces. This should help to reduce regulatory fragmentation between Member States and promote both technical and normative interoperability between enhanced digital services, while preserving fundamental rights.

3. Recognising the importance of, and strengthening, civil society organisations

Civil society organisations (CSOs) can be important actors endorsing and promoting core values such as democracy, the rule of law and solidarity, across the European Union. They can be part of wider coalitions of engagement in the context of human rights and new digital technologies, at times also providing a bridge between human rights experts, policy makers and technology experts. Civil society organisations can also facilitate online interaction between citizens and decision-makers to enhance the connection between the civic input and the political arena. Member States should implement measures to strengthen public awareness of the important role of CSOs, support CSOs and protect their role in the public sphere.

4. Protecting and empowering journalists and other media professionals

Today, fewer people obtain their news from independent quality-controlled media and more so from social media platforms. This, in turn, gives rise to echo chambers and filter bubbles, and to the isolation and polarisation of people. The shared reality in which we live is narrowed, and we are split into ever smaller and more fragmented groups of like-minded individuals.

Independent and trustworthy journalism remains of key importance for democracies in the digital era. We call upon governments to ensure the protection, safety, independence and empowerment of journalists and other media professionals, also acknowledging the important role of think tanks and other civil society organisations in promoting a reflective and informed political debate and in opinion-shaping. Strengthening media and improving journalism standards includes making available sufficient public funding and supporting programmes for quality fact-checking services and credibility indices**.**

We also endorse Civil Society Europe's recommendation to set up an early warning mechanism that enables journalists and other civil society actors to submit

complaints in a simple and non-bureaucratic manner on developments relevant to democracy, rule of law and civic space.[67]

5. Designing and regulating technologies for democracy – Democracy in and by design

5.1. Policies to ensure that technology development adheres to fundamental values

Digital technologies can and should be instruments for strengthening democracy, widening the public space, acting as a vehicle for direct and inclusive participation in public life, as well as bringing people together and fostering social cohesion. Their development should comply with core ethical values which include respect for the rule of law and for fundamental rights, with due regard to dignity, equality, welfare and freedom. Policy intervention is required to ensure through binding norms, as well as incentives and other measures, that technology development and deployment in the public and private sector adheres to fundamental values.

5.2. Policies to realise and safeguard privacy in a wider sense

One of the major concerns in the digital age is the protection of personal data and privacy, which must be understood as something broader than merely an individual right to freedom from undue interference. Privacy is also a right of people to have the space and opportunity to freely develop and express themselves. This places obligations on policy makers at all levels to secure that such space and opportunity exists, e.g. by issuing legislation to ensure that data about our lives and bodies are not collected without our knowledge and used to control and harm us, or legislation discouraging opt-out practices in personal data processing, as they do not leave sufficient space of free choice to data subjects compared to the opt-in standard of informed consent. This, in turn, requires that citizens – both individually and collectively – have a say in how data is used, for whose benefit and at whose cost. Simple compliance with informed consent, which places a high level of responsibility on the data subject with regard to the assessment of risks of data processing and its justification, is no longer sufficient to simultaneously promote access and guarantee privacy, nor functional in the light of novel ways to extract personal data (i.e. biometric tracking). Those who opt out of being datafied must not be disadvantaged in their ability to satisfy their basic needs. In addition, a right to non-datafication should be considered. In this regard we recommend that public funding is made available for public education and debate.

[67] Civil Society Europe, *Preliminary Proposals from Civil Society*, October 2022

5.3. Value-sensitive technology design can complement the protection of fundamental values

In addition to strengthening fundamental values by law and policy measures, respect for fundamental values can also be realised by value-by-design initiatives, which seek to protect various values, such as privacy, fairness or inclusivity. This means that privacy-protecting solutions should be designed into the hardware and the software of new (and revisited existing) technologies, adopting an ethics-by-design approach. Such a solution can also help to integrate legal and ethical trade-offs into technical infrastructures, and thus also provide a normative governance framework for data processing.

6. Democracy, technologies and the common good

6.1. Wider measures need to be taken to make sure that publicly funded innovation benefits the public

There is a strong misalignment between research and innovation funding and knowledge transfer into tangible benefits for the public: the openness of research, data and science has not been enough to ensure that society benefits from data use that was made possible through the activities of individuals and public infrastructures. We recommend that more measures are taken to ensure that innovation funded with public money in the European Union remains in the public sphere, and that commercial companies are given incentives to invest in the strengthening of the public sphere even if that does not offer them immediate commercial profits.

6.2. Safeguarding basic needs from market rationales

Digital technologies are strongly controlled by Big Tech corporations. Their expansionism from their original sphere of activity to new sectors threatens public control and citizens' sovereignty, deepening dependencies on private technology corporations for the provision of basic public goods. Democratic governments are losing their grip on basic public functions. The provision of public goods – such as healthcare, social security and public administrative services in general, education, employment, but indeed importantly also everything needed for a functioning democracy – should be kept away from market rationales and dynamics, remaining widely available and accessible to all independent of their ability to pay. This is a shared responsibility of all countries in the European Union.

The focus on markets turns individuals into consumers and reduces companies to mere market competitors. Strengthening democracies in the digital era, by contrast, requires understanding fairness not just as market fairness but as fairness in and across all domains, and ensuring that people's basic needs do not need to be met on market terms.

6.3. Public Private Partnerships (PPPs) as Public Private People Partnerships (PPPPs) should be designed to strengthen fundamental values

Collaborations between the public sector and technology corporations providing digital services should be established with care. Currently, profits generated by collaborations with tech corporations do not flow back to the public sector in equitable ways. Conditions that ensure a fair distribution of profits (monetary or other) should be predefined. Additional conditions for collaboration should take into account impacts that can be incremental and evident only at a later stage, such as the gradual reshaping of sectors and growing dependencies on private computational infrastructure.

7. Extending diplomacy: Valuing democracy, for people and planet

Digital technologies have been used for repression and control in third countries as well. Digital authoritarianism must be acknowledged as a geopolitical issue, eroding democracy as well as fundamental rights and the values and principles upon which these are based.

The European Union should make the fight against anti-democratic developments and repression a more central part of its high-level diplomacy and geopolitical strategies, developing a toolbox for dealing with the specific challenges also of digital repression, incorporating them fully into foreign policy instruments.

In this context, it should seize the opportunity and take seriously the responsibility to work towards a common international awareness of shared values and goals – as well as vulnerabilities. Europe's democracies support and sustain this awareness, and have been calling for increased efforts to take into account present and future generations, to care for the environment and the diversity of forms of life on Earth, to act upon climate change, and to realise sustainable ways of inhabiting the planet. Democracy should be valued as the best mean to identify common challenges and goals and to work towards achieving those goals together, also crucially beyond the EU's borders.

BIBLIOGRAPHY

Aizenberg, E. and Van Den Hoven, J., 2020. Designing for human rights in AI. Big Data & Society, 7(2), p.2053951720949566.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A. and Rieke, A., 2019. Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes. Proceedings of the ACM on human-computer interaction, 3(CSCW), pp.1-30.

Alonso, S., Keane, J. and Merkel, W. (eds.), 2011. The future of representative democracy. Cambridge University Press.

Amnesty International, 2021. Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms. https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/

Arendt, H., 1974. Interview with Roger Errera. https://www.nybooks.com/articles/1978/10/26/hannah-arendt-from-an-interview/

Bader, V., 2001. Associative democracy and the incorporation of minorities: Critical remarks on Paul Hirst's associative democracy. Critical Review of International Social and Political Philosophy, 4(1), pp.187-202.

Baptista, J.P. and Gradim, A., 2022. Who Believes in Fake News? Identification of Political (A) Symmetries. Social Sciences, 11(10), p.460.

Bedginfield, W., 2020. Everything that went wrong with the botched A-Levels algorithm. Wired, https://www.wired.co.uk/article/alevel-exam-algorithm

Bender, E.M., Gebru, T., McMillan-Major, A. and Shmitchell, S., 2021. On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In: Proceedings of the 2021 ACM conference on fairness, accountability, and transparency (pp. 610-623).

Bender, E.M. and Koller, A., 2020. Climbing towards NLU: On meaning, form, and understanding in the age of data. In: Proceedings of the 58th annual meeting of the association for computational linguistics (pp. 5185-5198).

Bertuzzi, L., 2023. AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices. EurActive, https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliaments-crunch-time-on-high-risk-categorisation-prohibited-practices/

Birch, K., Chiappetta, M. and Artyushina, A., 2020. The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset. Policy studies, 41(5), pp.468-487.

Birch, K. and Muniesa, F. (eds.), 2020. Assetization: turning things into assets in technoscientific capitalism. MIT Press.

Blum, C. and Zuber, C.I., 2016. Liquid democracy: Potentials, problems, and perspectives. Journal of political philosophy, 24(2), pp.162-182.

Boggs, C., 2011. Phantom democracy: Corporate interests and political power in America. Springer.

Buolamwini, J. and Gebru, T., 2018, January. Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency (pp. 77-91). PMLR.

Boulianne, S., 2020. Twenty years of digital media effects on civic and political participation. Communication research, 47(7), pp.947-966.

Bradley, S.H., Hemphill, S., Markham, S. and Sivakumar, S., 2022. Healthcare systems must get fair value for their data. BMJ 2022; 377:e070876.

Brake, D.R., 2014. Are we all online content creators now? Web 2.0 and digital divides. Journal of Computer-Mediated Communication, 19(3), pp.591-609.

Brown, A., 2001. Ten Years After the Soviet Breakup: From Democraticization to Guided Democracy. Journal of Democracy, 12(4), pp.35-41.

Calhoun, B., 2012. Shaping the public sphere: English coffeehouses and French salons and the age of the enlightenment. Colgate Academic Review, 3(1).

Chandwaney, A., 2020. After nearly 5 1/2 years, today is my last day at Facebook, https://www.facebook.com/ashok.chandwaney/posts/10220971727956399

Charter of fundamental rights of the European Union, 2012. Official Journal of the European Union, C83. Vol. 53, http://data.europa.eu/eli/treaty/char_2012/oj

Chueri, J., 2022. An emerging populist welfare paradigm? How populist radical right-wing parties are reshaping the welfare state. Scandinavian Political Studies, 45(4), pp.383-409.

Chueri, J., 2023. What distinguishes radical right welfare chauvinism? Excluding different migrant groups from the welfare state. Journal of European Social Policy, 33(1), pp.84-100.

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W. and Starnini, M., 2021. The echo chamber effect on social media. Proceedings of the National Academy of Sciences, 118(9), p.e2023301118.

Civil Society Europe & Philea, April 2023. Joint Civil Society Contribution to the Defence of Democracy Package. http://civilsocietyeurope.eu/we-need-a-new-pillar-on-civil-society-to-defend-democracy/

Civil Society Europe & Philea, October 2022. The Defence of Democracy Package: Building a Resilient Democracy and a strong and vibrant civic space – Preliminary Proposals from Civil Society. http://civilsocietyeurope.eu/wp-content/uploads/2022/10/The-Defence-of-Democracy-Package-Proposals-from-Civil-Society-1.pdf

CJEU (Court of Justice of the European Union) Judgement of 6 October 2015. Maximillian Schrems v Data Protection Commissioner, Case C-362/14. ECLI:EU:C:2015:650.

CJEU Judgment of 15 June 2021. Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit, Case C-645/19. ECLI:EU:C:2021:483.

CJEU Judgment of 16 July 2020. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18. ECLI:EU:C:2020:559.

CJEU Judgment of 10 July 2008. Centrum voor gelijkheid van kansen en voor racismebestrijding v Firma Feryn NV, Case C-54/07. ECLI:EU:C:2008:397.

Chueri, J., 2022. An emerging populist welfare paradigm? How populist radical right-wing parties are reshaping the welfare state. Scandinavian Political Studies, 45(4), pp.383-409.

Cohen, J.E., 2019. Between truth and power. Oxford University Press.

Cohen, J.E., 2013. What privacy is for. Harvard law review, 126(7), pp.1904-1933.

Copeland, R., 2019. Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans. The Wall Street Journal, https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services. OJ L 373, 21.12.2004, p. 37–43. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004L0113

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin. OJ L 180 , 19/07/2000, p. 22–26. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:HTML

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation. OJ L 303, 2.12.2000, p. 16–22. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078

Council of Europe, European Committee on Democracy and Governance (CDDG), 2021. Study on the impact of digital transformation on democracy and good governance. https://rm.coe.int/study-on-the-impact-of-digital-transformation-on-democracy-and-good-go/1680a3b9f9

Council of Europe, Committee on Bioethics (DH-BIO), 2019. Guide to public debate on human rights and biomedicine. Council of Europe, https://www.coe.int/en/web/bioethics/public-debate

Council of Europe, 128th Session of the Committee of Ministers, Elsinore (DK), 17-18 May 2018. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (ETS No. 108, 28.01.1981). https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

Delouya, S., 2022. Meta is being sued for giving US hospitals a data-tracking tool that allegedly ended up disclosing patient information to Facebook. Business Insider India, https://www.businessinsider.in/tech/news/meta-is-being-sued-for-giving-us-hospitals-a-data-tracking-tool-that-allegedly-ended-up-disclosing-patient-information-to-facebook/articleshow/93309108.cms

Dewey, J., 1939. Creative Democracy: The Task Before Us. In: John Dewey and the Promise of America, Progressive Education Booklet No. 14, Columbus, Ohio: American Education Press.

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast). OJ L 204, 26.7.2006, p. 23–36. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0054

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast). OJ L 204, 26.7.2006, p. 23–36, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0054

Dolan, K.A., 2022. Exclusive: Google Cofounder Sergey Brin Has Quietly Donated More Than $1 Billion Toward Parkinson's Disease. Forbes, https://www.forbes.com/sites/kerryadolan/2022/12/09/exclusive-google-cofounder-sergey-brin-has-quietly-donated-more-than-1-billion-toward-this-one-specific-disease/?sh=2b3e8a2d4d59

Dryzek, J.S., 1996. Democracy in Capitalist Times: Ideals, Limits, and Struggles. Oxford: Oxford University Press.

Ebers, M., Hoch, V., Rosenkranz, F., Ruschemeier, H. and Steinrötter, B., 2021. Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf – Eine kritische Bewertung durch Mitglieder der Robotics & AI Law Society (RAILS). RDi 2021, Heft 11, S. 528-537.

Ellis, E. and Watson, P., 2012. EU anti-discrimination law. OUP Oxford.

Eubanks, V., 2018. Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

European Commission, Protection of databases, https://digital-strategy.ec.europa.eu/en/policies/protection-databases

European Commission, 2023. Proposal for a Regulation establishing the Union Secure Connectivity Programme for the period 2023-2027 ('infrastructure for Resilience, Interconnection and Security by Satellite'- IRIS). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0057

European Commission, 2022a. Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (COM(2022) 68 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068

European Commission, 2022b. Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023-2027 (COM/2022/57 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0057

European Commission, 2022c. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM/2022/496 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496

European Commission, 2021a. 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 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

European Commission, 2021b. Recommendation (EU) 2021/1534 of 16 September 2021 on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union. OJ L 331, 20.9.2021, p. 8–20. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021H1534

European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, 2019a. The scale and impact of industrial espionage and theft of trade secrets through cyber. https://data.europa.eu/doi/10.2873/48055

European Commission, Joint Research Centre (JRC), 2019b. Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda. https://publications.jrc.ec.europa.eu/repository/handle/JRC116009

European Commission, 2016. The European Digital Competence Framework for Citizens, https://ec.europa.eu/social/BlobServlet?docId=15688&langId=en

European Commission, 2008. Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation (COM/2008/0426 final). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52008PC0426

European Commission, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 1998. Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) (XV D/5032/98). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf

European Convention on Human Rights, First Additional Protocol, 1952. https://www.echr.coe.int/Documents/Convention_ENG.pdf

European Council Conclusions, 22-23 March 2018. https://www.consilium.europa.eu/en/meetings/european-council/2018/03/22-23/

European Declaration on Digital Rights and Principles for the Digital Decade, 2022. https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration

European Economic and Social Committee, 2020. Finding a new consensus on European civil society values and their evaluation. https://www.eesc.europa.eu/sites/default/files/files/qe-01-20-495-en-n.pdf

European Group on Ethics in Science and New Technologies (EGE), 2022. Statement on Values in times of crisis: Strategic crisis management in the EU. European Commission, Directorate-General for Research and Innovation, Publications Office, https://op.europa.eu/en/publication-detail/-/publication/39416607-6bc5-11ed-9887-01aa75ed71a1/

European Group on Ethics in Science and New Technologies (EGE), 2021. Values for the Future: The role of ethics in European and global governance. European Commission, Directorate-General for Research and Innovation, Publications Office, https://op.europa.eu/en/publication-detail/-/publication/849e7ec4-cf13-11eb-ac72-01aa75ed71a1/language-en/format-PDF/source-245102876

European Group on Ethics in Science and New Technologies (EGE), 2018. Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. European Commission, Directorate-General for Research and Innovation, Publications Office, https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1/language-en/format-PDF/source-78120382

EGE hearing of 26/10/2022. Presentation of the European Commission's Directorate-General for Research and Innovation Unit D4.

European Parliament, 2021a. Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes (update). https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf

European Parliament, 2021b. Digital technologies as a means of repression and social control. Study requested by the DROI Subcommittee. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf

European Parliament, 2019. Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. Study requested by the LIBE Committee. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

European Parliament resolution of 17 April 2020 on EU coordinated action to combat

the COVID-19 pandemic and its consequences (2020/2616(RSP)). OJ C 316, 6.8.2021, p. 2–11, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020IP0054

European Parliament resolution of 15 June 2017 on online platforms and the digital single market. OJ C 331, 18.9.2018, p. 135–145. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52017IP0272

European Parliamentary Research Service, 2020. The practice of democracy: A selection of civic engagement initiatives. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/651970/EPRS_STU(2020)651970_EN.pdf

European Parliamentary Research Service, 2018. Prospects for e-democracy in Europe. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603213/EPRS_STU(2018)603213_EN.pdf

Federal Government of Germany, 2021. On the Application of International Law in Cyberspace - Position Paper. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Fitzgerald, M. and Crider, C., 2020. Under pressure: UK government releases NHS COVID data deals with big tech. openDemocracy.

Foa, R.S. and Mounk, Y., 2017. The signs of deconsolidation. Journal of democracy, 28(1), pp.5-15.

Fraser, N., 1992. Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. In: C. Calhoun (eds.), Habermas and the Public Sphere (pp. 109-142). MIT Press.

Freelon, D., Marwick, A. and Kreiss, D., 2020. False equivalencies: Online activism from left to right. Science, 369(6508), pp.1197-1201.

Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R. and Peissl, W., 2017. Surveillance, privacy and security. Taylor & Francis.

Frischlich, L., Hellmann, J.H., Brinkschulte, F., Becker, M. and Back, M.D., 2021. Right-wing authoritarianism, conspiracy mentality, and susceptibility to distorted alternative news. Social Influence, 16(1), pp.24-64.

Fundamental Rights Agency of the European Union (FRA), 2022. Bias in Algorithms – Artificial Intelligence and Discrimination. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf

Gibbons, B., 2020. Most MPs studied for university degrees now classed as 'low value' by UK Government. Get Surrey, https://www.getsurrey.co.uk/news/uk-world-news/most-mps-studied-university-degrees-18646647

Goldberg, J., 2020. Why Obama fears for our democracy. The Atlantic, https://www.theatlantic.com/ideas/archive/2020/11/why-obama-fears-for-our-democracy/617087/

Gorokhovskaia, Y., Shahbaz, A.., Slipowitz, A., 2023. Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy. Freedom House, https://freedomhouse.org/report/freedom-world/2023/marking-50-years

Gould, M., Joshi, I. and Tang, M., 2020. The power of data in a pandemic. Technology in the NHS Blog, 28.

Gray, M.L. and Suri, S., 2019. Ghost work: How to stop Silicon Valley from building a new global underclass. Eamon Dolan Books.

Habermas, J., 2022. Reflections and hypotheses on a further structural transformation of the political public sphere. Theory, Culture & Society, 39(4), pp.145-171.

Hanitzsch, T., Van Dalen, A. and Steindl, N., 2018. Caught in the nexus: A comparative and longitudinal analysis of public trust in the press. The international journal of press/politics, 23(1), pp.3-23.

Hartley, S., Raman, S., Smith, A. and Nerlich, B., 2018. Science and the politics of openness: Here be monsters (p. 352). Manchester University Press.

Heckelei, N., 2016. Simulierte Demokratie. Books on Demand.

Hinds, J., Williams, E.J. and Joinson, A.N., 2020. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies, 143, p.102498.

Hirst, P., 1996. Associative democracy—a comment on David Morgan. The Australian and New Zealand journal of sociology, 32(1), pp.20-26.

Information Commissioner's Office of the United Kingdom, 2017. RFA0627721 – provision of patient data to DeepMind. https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf

Ingelgom, V. for European Commission, Directorate-General for Research and Innovation, 2023. Research on deliberative and participatory practices in the EU. Publications Office of the European Union, https://data.europa.eu/doi/10.2777/936254

IPSOS Global Advisor, 2019. Trust in the media. IPSOS, https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/global-advisor-trust-in-media-2019.pdf

Keane, J., 2017. When trees fall, monkeys scatter: Rethinking democracy in China. World Scientific Publishing Europe Ltd., London.

Kelsen, H., 1920. Vom Wesen und Wert der Demokratie. Mohr. (English version: Kelsen, H. (author), Urbinati, N. and Invernizzi Accetti, C. (eds), 2013. The essence and value of democracy. Rowman & Littlefield.)

Kickbusch, I., Piselli, D., Agrawal, A., Balicer, R., Banner, O., Adelhardt, M., Capobianco, E., Fabian, C., Gill, A.S., Lupton, D. and Medhora, R.P., 2021. The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world. The Lancet, 398(10312), pp.1727-1776.

Killeen, M., 2022. Digital citizenship: A new proposal for an inclusive future. EurActive, https://www.euractiv.com/section/digital/news/digital-citizenship-a-new-proposal-for-an-for-inclusive-future/

Kofman, A. and Tobin, A., 2020. Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement. ProPublica, https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement

Kuhlmann, S. and Trute, H.H., 2022. Die Regulierung von Desinformationen und rechtswidrigen Inhalten nach dem neuen Digital Services Act. GSZ 2022, S. 115-122.

Kunig, P., 2008. Intervention, Prohibition of. In: Max Planck Encyclopedia of Public International Law.

Landemore, H., 2017. Deliberative democracy as open, not (just) representative democracy. Daedalus, 146(3), pp.51-63.

Larkin, B., 2013. The politics and poetics of infrastructure. Annual review of anthropology, 42, pp.327-343.

Ledford, H., 2019. Millions of black people affected by racial bias in health-care algorithms. Nature 574, 608-609.

Leetaru, K., 2018. Should Social Media Be Allowed To Profit From Terrorism And Hate Speech? Forbes, https://www.forbes.com/sites/kalevleetaru/2018/12/14/should-social-media-be-allowed-to-profit-from-terrorism-and-hate-speech/

Leonelli, S., 2023. Philosophy of Open Science. Cambridge, UK: Cambridge University Press.

Levitsky, S. and Ziblatt, D., 2019. How democracies die. Crown.

Lesher, M., Pawelec, H. and Desai, A., 2022. Disentangling untruths online: Creators, spreaders and how to stop them. OECD Going Digital Toolkit Notes, No. 23, Paris: OECD Publishing.

Lorenz-Spreen, P., Oswald, L., Lewandowsky, S. and Hertwig, R., 2023. A systematic review of worldwide causal and correlational evidence on digital media and democracy. Nature human behaviour, 7(1), pp.74-101.

Maki, K., 2011. Neoliberal deviants and surveillance: Welfare recipients under the watchful eye of Ontario Works. Surveillance & Society, 9(1/2), pp.47-63.

Marcus, G., 2022. AI Platforms like ChatGPT Are Easy to Use but Also Potentially Dangerou. Scientific American, https://www.scientificamerican.com/article/ai-platforms-like-chatgpt-are-easy-to-use-but-also-potentially-dangerous/

Mazzucato, M., 2021. Mission economy: A moonshot guide to changing capitalism. Penguin UK.

McGoey, L., 2015. No such thing as a free gift: The Gates Foundation and the price of philanthropy. Verso Books.

McMahon, A., Buyx, A. and Prainsack, B., 2020. Big data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. Medical law review, 28(1), pp.155-182.

Meijer, A.J., Curtin, D. and Hillebrandt, M., 2012. Open government: connecting vision and voice. International review of administrative sciences, 78(1), pp.10-29.

Molnár-Gábor, F., Beauvais, M.J., Bernier, A., Jimenez, M.P.N., Recuero, M. and Knoppers, B.M., 2022. Bridging the European Data Sharing Divide in Genomic Science. Journal of Medical Internet Research, 24(10), p.e37236.

Morrison, S.L. and Gomez, R., 2014. Pushback: Expressions of resistance to the "evertime" of constant online connectivity. First Monday.

Molnár-Gábor, F., 2016. Data Protection. In: Max Planck Enyclopedia of Comparative Constitutional Law, OUP.

Mouffe, C., 2000. Deliberative democracy or agonistic pluralism. https://www.ssoar.info/ssoar/handle/document/24654

Mudde, C. and Kaltwasser, C.R., 2017. Populism: A very short introduction. Oxford University Press.

Muldoon, J. and Booth, D., 2022. Socialist democracy: Rosa Luxemburg's challenge to democratic theory. Philosophy & Social Criticism, p.01914537221107403.

Müller, A., 2022. Sachverständigenstellungsnahme zur EU-Verordnung zu Künstlicher Intelligenz unter Einbeziehung von Wettbewerbsfähigkeit im Bereich Künstlicher Intelligenz und Blockchain-Technologie. Deutscher Bundestag, Ausschuss für Digitales, https://www.bundestag.de/resource/blob/911730/72880d80a804af16b5a69141ac8b2948/Stellungnahme-Mueller-data.pdf

Naeem, M., 2019. Uncovering the Enablers, Benefits, Opportunities and Risks for Digital Open Government (DOG): Enablers, Benefits, Opportunities and Risks for DOG. International Journal of Public Administration in the Digital Age 6(3).

Nagenborg, M., 2009. Designing spheres of informational justice. Ethics and information technology, 11(3), pp.175-179.

Nemitz, P., 2018. Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), p.20180089.

Nissenbaum, H., 2011. A contextual approach to privacy online. Daedalus, 140(4), pp.32-48.

Norton, A., 2023. Wild Democracy: Anarchy, Courage, and Ruling the Law. Oxford University Press.

Pasquale, F., 2016. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.

Paxton, M., 2019. Agonistic democracy: Rethinking political institutions in pluralist times. Routledge.

Pinker, S., 2015. The moral imperative for bioethics. The Boston Globe, https://www.bostonglobe.com/opinion/2015/07/31/the-moral-imperative-for-bioethics/JmEkoyzlTAu9oQV76JrK9N/story.html

Powles, J. and Hodson, H., 2018. Response to deepmind. Health and Technology, 8(1-2), pp.15-29.

Powles, J. and Hodson, H., 2017. Google DeepMind and healthcare in an age of algorithms. Health and technology, 7(4), pp.351-367.

Prainsack, B., El-Sayed, S., Forgó, N., Szoszkiewicz, Ł. and Baumer, P., 2022. Data solidarity - White paper. Growing up in a Digital World, The Lancet and Financial Times Commission. https://www.governinghealthfutures2030.org/wp-content/uploads/2022/12/DataSolidarity.pdf

Prainsack, B., 2017. Personalized medicine. In: Personalized Medicine. New York University Press.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). OJ L 277, 27.10.2022, p. 1–102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014

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 (Cybersecurty Act). OJ L 151, 7.6.2019, p. 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Reilly, S., 2018. Direct democracy: A double-edged sword. Lynne Rienner Publishers.

Reporters Without Borders, 2022. 20th World Press Freedom Index. https://rsf.org/en/rsf-s-2022-world-press-freedom-index-new-era-polarisation-0

Robinson, L., Cotten, S.R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Schulz, J., Hale, T.M. and Stern, M.J., 2015. Digital inequalities and why they matter. Information, communication & society, 18(5), pp.569-582.

Rosenblum, N.L. and Muirhead, R., 2019. A lot of people are saying: The New Conspiracism and the Assault on Democracy. Princeton University Press.

Runciman, D., 2018. How democracy ends. Profile Books.

Sandel, M.J., 2000. What money can't buy: the moral limits of markets. Tanner Lectures on Human Values, 21, pp.87-122.

Sapiezynski, P., Ghosh, A., Kaplan, L., Rieke, A. and Mislove, A., 2022. Algorithms that "Don't See Color": Measuring Biases in Lookalike and Special Ad Audiences. In: Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (pp. 609-616).

Savaget, P., Chiarini, T. and Evans, S., 2019. Empowering political participation through artificial intelligence. Science and Public Policy, 46(3), pp.369-380.

Schmidt, R., 2021. Grenzenlose Souveränität im Cyberspace: Eine Kritik des Positionspapiers der Bundesregierung zum digitalen Völkerrecht. Verfassungsblog.

Schuman, R., 1964. Pour l'Europe. Nagel, https://www.schuman.info/democracy.htm

Sen, A. (2009). Development as Freedom. Knopf.

Sesing, A. and Tschech, A., 2022. AGG und KI-VO-Entwurf beim Einsatz von Künstlicher Intelligenz. MMR–Zeitschrift für IT-Recht und Recht der Digitalisierung, 25, pp.24-30.

Shapiro, I. and Macedo, S. (eds.), 2000. Designing democratic institutions (Vol. 42). NYU Press.

Sides, J., 2015. Why Congress should not cut funding to the social sciences. The Washington Post, https://www.washingtonpost.com/news/monkey-cage/wp/2015/06/10/why-congress-should-not-cut-funding-to-the-social-sciences/

Sharon, T., 2022. Beyond privacy: there are wider issues at stake over Big Tech in medicine. Open Democracy, https://www.opendemocracy.net/en/technology-and-democracy/beyond-privacy-there-are-wider-issues-at-stake-over-big-tech-in-medicine/

Sharon, T., 2021a. From hostile worlds to multiple spheres: towards a normative pragmatics of justice for the Googlization of health. Medicine, Health Care and Philosophy, 24(3), pp.315-327.

Sharon, T., 2021b. Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. Ethics and Information Technology, 23(Suppl 1), pp.45-57.

Soron, D. and Laxer, G., 2006. Thematic introduction: Decommodification, democracy and the battle for the commons. Not For Sale: Decommodifying of public life, pp.15-37.

Spitale, G., Biller-Andorno, N. and Germani, F., 2023. AI model GPT-3 (dis) informs us better than humans. arXiv:2301.11924.

Spitale, G., Germani, F. and Biller-Andorno, N., 2023. The PHERCC matrix. An ethical framework for planning, governing, and evaluating risk and crisis communication in the context of public health emergencies. Am J Bioeth, 4, pp. 1-16.

Spitale, G., Merten, S., Jafflin, K., Schwind, B., Kaiser-Grolimund, A. and Biller-Andorno, N., 2021. A novel risk and crisis communication platform to bridge the gap between policy makers

and the Public in the Context of the COVID-19 Crisis (PubliCo): protocol for a mixed methods study. JMIR research protocols, 10(11), p.e33653.

Staab, P., 2019. Digital Capitalism: Market and Hegemony in the Economy of Superabundance. Suhrkamp.

Steiger, D., 2021. Wehrhafte Demokratie im digitalen Zeitalter: Völkerrechtliche Grenzen in- und ausländischer Einflussnahme auf Wahlen. In: Die Herausforderungen der digitalen Kommunikation für den Staat und seine demokratische Staatsform (The Challenges of Digital Communication for the State and its Democratic State Form) (pp. 137-162). Nomos Verlagsgesellschaft mbH & Co. KG.

Steiner, G., 2015. The idea of Europe: an essay. Abrams.

Strøm, K., Müller, W.C. and Bergman, T. (eds), 2003. Delegation and Accountability in Parliamentary Democracies, Comparative Politics. Oxford University Press.

Surden, H., 2007. Structural Rights in Privacy. MU Law Review 60: 1605-1629.

Taylor, P.L., 2009. Scientific self-regulation—So good, how can it fail? Commentary on "The problems with forbidding science". Science and Engineering Ethics, 15, pp.395-406.

Tech Transparency Project, 2023. Meta Creates Pages for ISIS, Undermining Anti-Terrorism Efforts, https://www.techtransparencyproject.org/articles/meta-creates-pages-for-isis-undermining-anti-terrorism-efforts

Thiel, T., 2023. A polarizing multiverse? Assessing Habermas' digital update of his public sphere theory. Constellations 30:69–76.

Tobler, C., 2005. Indirect discrimination: a case study into the development of the legal concept of indirect discrimination under EC law. Vol 10, Intersentia.

Törnberg, P., 2023. How platforms govern: Social regulation in digital capitalism. Big Data & Society, 10(1), p.20539517231153808.

Treaty on European Union. Official Journal C 326 , 26/10/2012 P. 0001 - 0390, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

Troncoso, C., Payer, M., Hubaux, J.P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D. and Barman, L., 2020. White paper on Decentralized Privacy-Preserving Proximity Tracing. https://nebelwelt.net/files/20DEB.pdf

Turow, J., Hennessy, M. and Draper, N., 2015. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. A Report from the Annenberg School for Communication, University of Pennsylvania.

United Nations Working Group on developments in the field of information and telecommunications in the context of international security, 2021. Final Substantive Report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

United Nations, 2019. Report of the Special Rapporteur on extreme poverty and human rights. General Assembly, https://undocs.org/A/74/493

Van Bekkum, M. and Borgesius, F.Z., 2021. Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security, 23(4), pp.323-340.

Van den Hoven, M.J., 1997. Privacy and the varieties of moral wrong-doing in an information age. Acm Sigcas Computers and Society, 27(3), pp.33-37.

Van Deursen, A.J. and Van Dijk, J.A., 2014. The digital divide shifts to differences in usage. New media & society, 16(3), pp.507-526.

Van Dijk, N., Casiraghi, S. and Gutwirth, S., 2021. The 'Ethification' of ICT Governance. Artificial Intelligence and Data Protection in the European Union. Computer Law & Security Review, 43, p.105597.

Voltaire, 1765. Collection des Lettres sur les Miracles ('Collection of Letters on Miracles'), letter no. 11.

Von Thadden, E., 2023. Ändert das Digitale den Kapitalismus? Die Zeit Online, https://www.zeit.de/2023/02/digitalisierung-demokratie-kapitalismus-philipp-staab

Walzer, M., 1983. Spheres of justice: A defense of pluralism and equality. Basic Books.

Wagner, B., 2018. Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping? In: Being profiled: COGITAS ERGO SUM - 10 Years of Profiling the European Citizen. Amsterdam University Press.

Walby, S., 2009. Globalization and inequalities: Complexity and contested modernities. Sage.

Warren, M., 1992. Democratic theory and self-transformation. American political science review, 86(1), pp.8-23.

Wei, L., 2012. Number matters: The multimodality of Internet use as an indicator of the digital inequalities. Journal of Computer-Mediated Communication, 17(3), pp.303-318.

Weil, E., 2023. You Are Not a Parrot And a chatbot is not a human. And a linguist named Emily M. Bender is very worried what will happen when we forget this. Intelligencer, https://nymag.com/intelligencer/article/ai-artificial-intelligence-chatbots-emily-m-bender.html

Whittaker, M., Alper, M., Bennett, C.L., Hendren, S., Kaziunas, L., Mills, M., Ringel Morris, M., Rankin, J.,Rogers, E., Salas, M., Myers West, S., 2019. Disability, Bias, and AI. AI Now Institute at NYU, https://ainowinstitute.org/disabilitybiasai-2019.pdf

Xu, X., Brennan, E. and Frater, J., 2023. EU bans TikTok from official devices across all three government institutions. https://edition.cnn.com/2023/02/28/tech/tiktok-eu-ban-intl-hnk/index.html

Yeung, K., Howes, A. and Pogrebna, G., 2020. AI Governance by Human Rights–Centered Design, Deliberation, and Oversight. The Oxford handbook of ethics of AI, pp.77-106.

York, J.C., 2022. Silicon values: The future of free speech under surveillance capitalism. Verso Books.

Zhuravskaya, E., Petrova, M. and Enikolopov, R., 2020. Political effects of the internet and social media. Annual review of economics, 12, pp.415-438.

Zuboff, S., 2021. The coup we are not talking about. The New York Times, https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html

Zuboff, S., 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs.

Zuiderveen Borgesius, F., 2018. Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

THE MEMBERS OF THE EGE

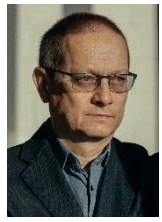
Barbara Prainsack
Chair of the EGE

Maria do Céu Patrão Neves
Vice-Chair of the EGE

Nils-Eric Sahlin
Vice-Chair of the EGE

Nikola Biller-Andorno

Migle Laukyte



Paweł Łuków

Pierre Mallia

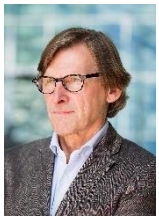
Fruzsina Molnár-Gábor

Thérèse Murphy

Herman Nys

Laura Palazzani

Tamar Sharon



Marcel Jeroen van den Hoven

Renata Veselská

Takis Vidalis

ACKNOWLEDGMENTS

The President of the European Commission, Ursula von der Leyen, addressed the EGE by letter in February 2023 to request this Opinion.

The development of the present Opinion involved several relevant services of the European Commission and, beyond, a wide range of stakeholders and experts, many of whom presented their perspectives to the EGE on the occasion of dedicated hearings. A central part of this, pursuant to Commission Decision 2021/156, was the Open Round Table, which was held on 29 March 2023. The event gathered an array of perspectives, from academia through to international organisations, industry and civil society organisations, to discuss the questions raised by recent technological advances as well as by longstanding tensions at the very heart of democracy. It provided a forum for dialogue, and an opportunity to gather inputs from experts and interested participants, to further the reflection and refine the EGE's recommendations.

All of the people who participated in the different phases of this process, be it physically or online or in writing, are appreciatively recognised. Notably: Julien Mousnier, Maria-Luisa Cabral, Toma Sutic, Roua Abbas, Martina del Ministro, Harry Panagopulos, Michalina Zięba, Susana Nascimento, Katja Reppel, Francisco de la Torre Francia, Julie Baleriaux, Laura Smillie, Laurent Bontoux, Andrea Accardo, David Kaye, Diego Naranjo, Michael Saward, Carlotta Besozzi, Paolo Benanti, Louise Edwards, Alison Weightman, Frederico Rocha, Rafael Carrascosa Marzo, Ole Petersen, and Elias Weiss.

The close and fruitful cooperation with the teams in the sister international organisations tasked with the ethics and governance of emerging technologies (notably: UNESCO, WHO, FAO, ILO, OHCHR, WTO, WIPO, UNEP, ICGEB as well as Council of Europe and OECD) is gratefully acknowledged, as is the crucial role in that regard of the UN Inter-Agency Committee on Bioethics, in which the European Commission is represented by Jim Dratwa. Appreciation is extended to the Chairs, Secretaries-General, and representatives of the National Ethics Councils emanating from the Member States of the EU. The exchanges with them in the context of the development of the Opinion have undoubtedly helped to refine the thinking therein. Similarly, appreciation is extended to the members of the European Commission's Interservice Group on Ethics and EU Policy.

THE EGE TEAM

Jim DRATWA
Head of the EGE Team

Barbara GIOVANELLI
Policy Officer

Marta JASINSKA
Policy Assistant

Contact: ec-ethics-group@ec.europa.eu

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union.
You can contact this service:

– by freephone: **00 800 6 7 8 9 10 11** (certain operators may charge for these calls),

– at the following standard number: **+32 22999696**,

– via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU Publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Recent years have seen profound challenges to democracy, including alarming populist and autocratic shifts. Democracy can quickly become an empty shell if it is not underpinned by fundamental rights and the values it seeks to protect and promote. In this context, the EGE examines how certain configurations of digital technologies can contribute to a weakening of democratic institutions, even if they may not be its sole cause. Among these are the spread of harmful information, an unduly narrow understanding of privacy, algorithmic surveillance, manipulation and discrimination, foreign interference, and the expansion of Big Tech into public sectors.

Against this background, the EGE conceptualises a 'thick' understanding of democracy, that considers it, beyond a political system, a wider social system that protects its own societal preconditions. The EGE also formulates a series of recommendations that may help to develop pathways for how this vision can, collectively and democratically, be further translated into reality. It stresses that strengthening democracy means safeguarding this very process.

Research and Innovation policy

Publications Office
of the European Union