

The Future of the (Digital) State

Lorenzo Casini*

ABSTRACT: Can the digital revolution transform the very idea of the state and its functioning? The article investigates the ways in which technologies are influencing public institutions and their functioning, with particular regard to the contemporary and ‘democratic’ model of the state that was established in the 20th century. A first group of influences concerns the modes of exercising sovereignty and, in particular, the fundamental functions of the state. Therefore, the techniques of so-called direct democracy and their limits in pursuing the utopia of law-making by the people, the use of algorithms by judges, and the increasing spread of automated administrative decisions are examined. A second group of conditioning refers to the effects that the technological revolution has on the other two elements of the state, the people and the territory. Issues concerning the protection of fundamental rights, border crises, the relationship between technology and information and, consequently, between democracy and truth are then analyzed. From these constraints emerges a model based on ‘surveillance’, in which big data, their use and protection have acquired a strategic role. A model whose spread has undoubtedly increased with the pandemic, but also highlighted its limits and possible countermeasures. The digital revolution, the dominant role of Big Tech and social network, and the increasing use of artificial intelligence are profoundly affecting public institutions and civil society: what is the future of the (digital) State?

KEYWORDS: State; digital revolution; algorithms; Artificial Intelligence; robot judges

SUMMARY: 1. The (democratic) state in the age of Google – 2. The technological challenge: the rise of algorithms – 2.1. Law-making by the people: the limits of direct democracy – 2.2. Robot judges? – 2.3. Automated administrative decisions – 3. A surveillance State? Privacy, walls, and democracy – 4. Technology and (dis)information – 5. What future for the digital state? – 5.1. The fate of big data: private v. public – 5.2. Institutions in the digital age: writing v. orality.

“Facebook defines who we are, Amazon defines what we want, and Google defines what we think.”¹

* Professor of Administrative Law, IMT School for Advanced Studies (Lucca, Italy). An earlier draft of this paper was presented at the European Public Law Group Annual Meeting (Legrainia, 15-16 September 2023). The author warmly thanks all the participants for their helpful suggestions. Mail: lorenzo.casini@imtlucca.it. *Contributo su invito.*

1. The (democratic) State in the age of Google

As of January 2023, the number of Internet users worldwide exceeded 5 billion: two out of three people now access the Internet (64.4% of the world's population, or 5.16 billion people), an increase of 6% compared to 2021. The increase in users of so-called social media is even faster: at the beginning of 2023 there were 4.75 billion people on social platforms, equal to 60% of the world's population, an increase of more than 10% compared to 2021 (561 million people).² There were 354 million Internet addresses (so-called domain names) at the end of 2022, when there were 160 million in 2008.³

Thousands of data and statistics highlight the extraordinary impact of the technological revolution on society, the economy, and culture. If one only sits in a public space with other people, will notice that almost everyone present – including children – is likely to be 'immersed' in their smartphone. And by now, the photographic medium, via mobile phone or tablet, has even become the main way of perceiving works of art: this is represented by the works of Giacomo Zaganelli in his 'Grand Turismo', exhibited in summer 2019 at the Uffizi Galleries, which reproduce the 'distortions' caused by digital technologies on visits to museums. The situation is not changing inside our homes: in 2018, for example, the value of the world market for so-called 'smart home' products, such as the Nest thermostat, was around \$36 billion; the estimate for 2028 is for a value five times greater, at over \$160 billion in total.⁴

The 2020 pandemic has further accelerated the use of technological tools in many areas, also imposing virtual forms of communication as an ordinary means of interaction: the number of users of some platforms has increased up to thirty times more than before (in the case of Zoom, for example, there were 10 million in December 2019 and already 300 million in 2020). Think of teaching or the meetings of collegiate bodies held online and no longer in the presence of others because of the need to contain contagion. In this case, technology has been a remedy that, however, has also greatly transformed the ways of teaching, arguing, and negotiating. This also explains why there has been much debate as to whether parliaments should be able to meet, debate and vote remotely, over and above security and confidentiality issues.

The widespread dissemination of information media and the ever-easier access to communication tools have called into question the very notions of government, state, and democracy,⁵ the 'crises' of

¹ G. DYSON, *Turing's Cathedral. The Origins of the Digital Universe*, Penguin, New York, 2012, 308, a phrase also taken up by F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard, 2015, 15.

² These are the figures from the *Global Digital 2022* report (<https://wearesocial.com/it/blog/2022/01/digital-2022-i-dati-globali/>). In 1997, there were approximately 120 million Internet users worldwide; in 2015, they exceeded 3 billion (<https://ourworldindata.org/internet>).

³ <https://dnib.com/articles/the-domain-name-industry-brief-q1-2023>.

⁴ For data, S. ZUBOFF, *The Age of Surveillance Capitalism*, London, 2019, and www.marketsandmarkets.com (see the Report on Smart Home Market, March 2023).

⁵ C.R. SUNSTEIN, *#republic. Divided Democracy in the Age of Social Media*, Princeton, 2017; T. BALDWIN, *Ctrl Alt Delete: How Politics and the Media Crashed our Democracy*, London, 2018; S. CASSESE, *La democrazia e i suoi limiti*, 2nd ed., Milan, 2018, in particular 111 ff, on 'electronic democracy'; J. BARTLETT, *The People Vs Tech. How*

which have been the subject of in-depth analysis from a legal and political perspective.⁶ This is because technology challenges even more the sovereignty of states, already tested by the emergence of global rules and markets. On the other hand, [n]o government, even the most totalitarian, has been able to arrest the flow or to resist the trend to push ever more of its operations into the digital domain. Most of the democracies have an ingrained instinct that an attempt to curtail the effects of an information revolution would be impossible and perhaps also immoral. Most of the countries outside the liberal-democratic world have set aside attempts to shut out these changes and turned instead to mastering them. Every country, company, and individual is now being enlisted in the technological revolution as either a subject or an object.⁷

The 2020 pandemic also represented, for some states, an opportunity to use technology to their advantage, in order to regain their position with respect to powers that have been eroded over time or limited by the assertion of fundamental rights: think of freedom of movement or border control. Nor can it come as a surprise that the conflict between Russia and Ukraine that broke out in February 2022 also saw, in the international sphere, a reaction of states supported by technological means: think of the block imposed on Russia on the digital banking payments system (the so-called Swift system, by the Society for Worldwide Interbank Financial Telecommunication).

Internet and social networks, however, still play a decisive political role in the world today: this is confirmed by the famous phrase of the founder and head of Facebook, now renamed Meta, Mark Zuckerberg, according to whom his company is, in many respects, “more like a government than a traditional company”.⁸ The numbers of the Facebook platform are impressive: in April 2023, the number of monthly active users exceeded 3 billion and continue to increase, albeit at a slower pace than a few years ago.⁹

A confirmation of the connections between new technologies and politics occurred in 2018, when the US Senate summoned the top executives of the major social media companies to a hearing to report on abuses in data management in connection with Russia’s disinformation activities during the 2016 US presidential election (the so-called “Cambridge Analytica” scandal).¹⁰

The images of the founder of Facebook, now Meta, being questioned by US senators have been seen all over the world and have made many realize the condition in which states find themselves today in the face of technology giants. The hundreds of questions and answers exchanged between the US senators and one of the richest and most influential men on the planet covered many topics: govern-

the Internet is Killing Democracy (and How We Save It), London, 2018, and *La datacratie*, in *Pouvoirs*, 2018, 164.

⁶ We only mention here, in addition to S. CASSESE, *La democrazia e i suoi limiti*, above, the volumes *Constitutional Democracy in Crisis?*, edited by M.A. GRABER, S. LEVINSON, M. TUSHNET, Oxford, 2018, Y. MENY, *Popolo ma non troppo. Il malinteso democratico*, transl. it., Bologna, 2019, and S. LEVITSKY, D. ZIBLATT, *How Democracies Die. What History Reveals About Our Future*, New York, 2018.

⁷ H. KISSINGER, *World Order*, New York, 2014, 343 ff.

⁸ Zuckerberg’s sentence is quoted in many articles and interviews: see, for example, <https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge>.

⁹ <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>.

¹⁰ See, in particular, the hearing of Mark Zuckerberg before the *United States Senate Committee on the Judiciary and the United States Senate Committee on Commerce, Science and Transportation*, 10 April 2018 (<https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data>).

ance and Internet rules, protection of personal data, foreign governments' interference in the democratic life of other countries, fake news, freedom of expression and censorship, the use of algorithms, artificial intelligence, and more. During the hearing, the Facebook founder also stated that his biggest concern at the time was "making sure that no one interferes in the various 2018 elections around the world."

The US presidential election in 2020 was once again a testing ground for the use of social networks in politics and by political figures. The challenge between the then outgoing President Donald Trump and the Democratic candidate Joe Biden saw the platforms intervene on several occasions with alerts or outright removal of posts or tweets deemed untrustworthy or in any case a source of unverified information. In particular, the allegations of fraud made by defeated Donald Trump in the election found an immediate curb from social media, which accompanied Trump's claims with *caveats* and clarifications. However, the highest point in the "subversive" use of social media in this affair occurred on 6 January 2021 when, on the occasion of the Capitol's assault in Washington by some supporters of outgoing President Trump, the latter's Facebook, Instagram and Twitter accounts were suspended. The parable of the relationship between social networks and electoral rounds, which reached perhaps its darkest moment on that occasion in 2020-21, is well illustrated by a former US President, Barack Obama, with reference to his campaign in 2008.¹¹

But can the new technologies not only profoundly condition the times and ways of life of contemporary societies and democracies, but also transform the very idea of the state, its concrete physiology and functioning?

In order to address this complex question, it is necessary to investigate the ways in which technologies are influencing public institutions and their functioning, with particular regard to the contemporary and 'democratic' model of the state that was established in the 20th century.¹² There are now numerous 'digital' influences on crucial profiles for the organization and activities of institutions and public administrations.¹³

A first group of constraints concerns the modes of exercising sovereignty and, in particular, the fundamental functions of the state. Therefore, the techniques of so-called direct democracy and their

¹¹ B. OBAMA, *A Promise Land*, New York, 2020, 130 ff.: "What struck me as well was the growing role that technology played in our victories. The extraordinary youth of my team allowed us to embrace and refine the digital networks that Howard Dean's campaign had set in motion four years earlier. Our status as upstarts forced us to trust, again and again, the energy and creativity of our internet-savvy volunteers. Millions of small donors were helping to fuel our operation, emailed links helped to spread our campaign messaging in ways that Big Media couldn't, and new communities were forming among people who'd previously been isolated from one another. Coming out of Super Tuesday, I was inspired, imagining that I was glimpsing the future, a resurgence of bottom-up participation that could make our democracy work again. What I couldn't fully appreciate yet was just how malleable this technology would prove to be; how quickly it would be absorbed by commercial interests and wielded by entrenched powers; how readily it could be used not to unify people but to distract or divide them; and how one day many of the same tools that had put me in the White House would be deployed in opposition to everything I stood for."

¹² For an in-depth discussion of these issues, see L. CASINI, *Lo Stato (im)mortale. Pubblici poteri e globalizzazione nell'era digitale*, Milan, 2022.

¹³ L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023. See also B. MARCHETTI, *L'amministrazione digitale*, in *Enciclopedia del diritto. I tematici*, III – *Le funzioni amministrative*, edited by B.G. MATTARELLA, M. RAMAJOLI, Milan, 2022, 75.

limits in pursuing the utopia of law-making by the people, the use of algorithms by judges, and the increasing spread of automated administrative decisions are examined.

A second group of conditioning refers to the effects that the technological revolution has on the other two elements of the state, the people and the territory. Issues concerning the protection of fundamental rights, border crises, the relationship between technology and information and, consequently, between democracy and truth are then analyzed. From these constraints emerges a model based on 'surveillance', in which big data, their use and protection have acquired a strategic role. A model whose spread has undoubtedly increased with the pandemic, but also highlighted its limits and possible countermeasures.

2. The technological challenge: the rise of algorithms

In September 2018, Twitter co-founder Jack Dorsey, during a hearing in the US Senate, acknowledged that large companies owning major social media should work together with states and, more generally, with public authorities. Dorsey, in particular, stated that "as a private company, there are threats that we cannot understand and address alone. We must continue to work together with our elected officials, government partners, industry peers, outside experts, and other stakeholders so that the American people and the global community can understand the full context in which these threats arise".¹⁴

On similar positions, Mark Zuckerberg finally expressed himself in March 2019. In his *op-ed* in the 'Washington Post', the Facebook founder publicly appealed to governments to intervene, together with his company, with 'new rules' in four priority areas: harmful content, election integrity, privacy, and data portability.¹⁵

The state is challenged by new technologies. Not least because to these challenges "[t]here is no nationalist answer. As in the case of climate change, so also with technological disruption, the nation state is simply the wrong framework to address the threat."¹⁶ In fact, the impact of the 'digital' on the state, and on democracy, is enormous. That is why many countries are gearing up. In France, for example, studies on so-called "datacratie" have flourished; in the United Kingdom, Jeremy Corbyn has presented a manifesto for digital democracy.¹⁷

In the age of Google, numerous issues emerge that the state and states must take care of, such as the idea of cyberspace as a global public good, the danger of decision-making processes dominated by algorithms, and the damage that fake news and disinformation can cause both to individuals and

¹⁴ The hearings of Jack Dorsey, Co-Founder and then Chief Executive Officer of Twitter, and Sheryl Sandberg, then Chief Operating Officer of Facebook, before the *US Senate Select Committee on Intelligence*, 5 September 2018 are available here: <https://www.intelligence.senate.gov/hearings/open-hearing-foreign-influence-operations-use-social-media-platforms-company-witnesses>.

¹⁵ M. ZUCKERBERG, *The Internet Needs New Rules. Let's Start in These Four Areas* (30 March 2019), in https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

¹⁶ Y.N. HARARI, *21 Lessons for the 21st Century*, London, 2018, 184.

¹⁷ The manifesto is available at [https://d3n8a8pro7vhm.cloudfront.net/corbynstays/pages/329/attachments/original/1472552058/Digital Democracy.pdf?1472552058](https://d3n8a8pro7vhm.cloudfront.net/corbynstays/pages/329/attachments/original/1472552058/Digital%20Democracy.pdf?1472552058).

to society as a whole. Technological advancement, on the other hand, has always prompted new representations of the state, ‘*machina machinarum*’,¹⁸ as happened in the past with other images: famous is that of the clock-state, a figure also evoked by Hobbes.¹⁹

But what are the relationships between the technological revolution and the state? How do the new information and communication technologies affect the sovereignty that “protects democracy”?²⁰ Could “the technological unification of the world” really lead to the “demise of the states system”?²¹ Technology is also largely used in public administrations: we can mention the €20,000 fine imposed in Sweden, back in 2019, against an educational institution that had adopted facial recognition tools for students for control purposes, in violation of European privacy regulations (and it was the first such penalty applied by the Swedes).²² Moreover, the use of blockchain and artificial intelligence (AI) by the public sphere is increasingly common: in the UK, the HM Land Registry, i.e. the land registry, has developed a form of smart contract using self-certifications via blockchain; in Estonia, this technology has been used since 2012 for the inheritance registry, while in the Netherlands it is being adopted in public welfare and assistance systems; in Argentina, an AI system for automated smart decision-making in the procurement sector has been active since 2018 (the Prometea system).²³ Finally, mention must be made of China, where at least since 2009, massive use has been made of AI for data collection and population monitoring purposes.²⁴

All these examples, beside their immediate implications regarding democracy and fundamental rights, also show the competition between law and digital technology, insofar as, precisely in the case of blockchain, it is a tool for certifying facts or situations and, if one thinks of the market for non-fungible tokens (NFT), authenticity. As has been noted, the blockchain “*lie par un acte technique une situation à un régime de vérité. Comme le langage en général et le concept en particulier, elle institue ce qui sera dorénavant considéré comme réel par un acte public, mais au lieu de nommer celui-ci, elle le code. La blockchain est par là un langage sans représentation du monde, à la grande différence du langage ordinaire, mais qui remplit les mêmes fonctions que le langage (nomination et jugement)*”.²⁵

¹⁸ N. IRTI, *Lo Stato: machina machinarum*, in *Rivista trimestrale di diritto pubblico*, 2004, 309 ff.

¹⁹ O. MAYR, *Authority, Liberty, and Automatic Machinery in Early Modern Europe*, London and Baltimore, 1986, 104 ff.

²⁰ D. GRIMM, *Sovereignty. The Origin and Future of a Political and Legal Concept* (2009), New York, 2015, 128.

²¹ It was already H. BULL, *The Anarchical Society: A Study of Order in World Politics*, London, 1977, 392 ff., who pointed out the relations between technological development and the fate of states.

²² https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en.

²³ These and other examples are reported by the Observatory on the Digital State of the Institute for Research on Public Administration (IRPA): <https://www.irpa.eu/category/stato-digitale/>.

²⁴ D. ACEMOGLU, S. JOHNSON, *Power and Progress. Our Thousand-Year Struggle Over Technology and Prosperity*, London, 2023, 340 ff.

²⁵ A. GARAPON, J. LASSÈGUE, *Justice digitale: Révolution graphique et rupture anthropologique*, Paris, 2018, 140 ff., here 142 (Author’s translation: “Through a technical act, it links a situation to a system of truth. Like language in general and the concept in particular, it institutes what will henceforth be considered as real by a public act, but instead of naming it, it codes it. In this way, blockchain is a language that does not represent the world, unlike ordinary language, but which performs the same functions as language (naming and judging)”). See also O.

Among the various areas in which the influence of new technologies on public powers emerges, it seems then possible to distinguish at least two groups of issues, also identified on the basis of the effects that digital conditioning produces on the constituent elements of the state, namely the people, the territory, and sovereignty.

A first group concerns the ways in which fundamental legislative, judicial, and executive-administrative functions are exercised. Thus, we will consider the techniques of so-called direct democracy and their limits; the use of algorithms by judges; automated decisions taken by public administrations.

The second group of issues, analyzed in the following paragraphs, relates to the changes taking place that have consequences for the people and the territory, with regard to three aspects: the protection of fundamental rights, in particular the protection of personal data; the border crisis; the relationship between technology and information and, therefore, between democracy and truth.

The study of both these subject groups shows the significant effects that technology has on the decision-making processes of institutions.²⁶ And it is in this area that the use of algorithms, including so-called predictive algorithms, to support the decisions of public authorities is becoming increasingly widespread: this is the case, for example, with justice and the calculation of punishment in criminal trials or, more generally, with the so-called profiling of citizens.²⁷

An algorithm is nothing more than a systematic scheme or process of calculation that enables a problem to be solved.²⁸ In its computer applications, the term identifies a sequence of instructions given to a machine for it to follow a certain procedure and thus produce a result. Then, depending on when these instructions are given and the intended procedure, there can be different types of algorithms: deterministic, probabilistic, machine learning, predictive.²⁹ When we search for a word on Google, for instance ‘car’, the search engine will use an algorithm to choose the results to show us; and it is always an algorithm that, shortly after our search, will cause us to receive by email or see advertisements related to cars on our social accounts.³⁰ Ultimately, algorithms are for computers like “recipes”, i.e. “a series of precise steps that can be followed mindlessly”: although “[t]here’s no equation to suggest a dress to wear, but an algorithm could easily be written for that-it will work its

POLLICINO, G. DE GREGORIO (eds.), *Blockchain and Public Law: Global Challenges in the Era of Decentralisation*, Cheltenham, 2021.

²⁶ This issue is examined by M. ZALNIERIUTE, L. BENNETT MOSES, G. WILLIAMS, *The Rule of Law and Automation of Government Decision-making*, in *Modern Law Review*, 72, 2019, 1 ff.

²⁷ K. CHAGAL-FEFERKORN, *The Reasonable Algorithm*, in *U. Ill. J.L. Tech. & Pol’y*, 2018, 111; J.A. KROLL *et al.*, *Accountable Algorithms*, in *U. Pa. L. Rev.*, 165, 2017, 633; F. PASQUALE, *The Black Box Society*, above; and D. CARDON, *Le pouvoirs des algorithmes*, in *La datacratie*, above, 63.

²⁸ P. DOMINGOS, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*, New York, 2015.

²⁹ G. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Naples, 2019, 5 ff.

³⁰ On artificial intelligence, M. BODEN, *AI. Its Nature and Future*, Oxford, 2018, and ID., *Artificial Intelligence. A Very Short Introduction*, Oxford, 2018. See also C. KERRIGAN (ed.), *Artificial Intelligence. Law and Regulation*, Cheltenham, 2022; J. DUBERRY, *Artificial Intelligence and Democracy. Risks and Promises of AI-Mediated Citizen-Government Relations*, Cheltenham, 2022; and W. BARFIELD, U. PAGALLO, *Research Handbook on Artificial Intelligence*, Cheltenham, 2022.

way through a series of either/or questions (morning or night, winter or summer, sun or rain), with each choice pushing to the next”.³¹

The diffusion of mechanisms for customizing the results of searches carried out online has brought to light the phenomenon of the so-called Filter Bubble, whereby these mechanisms, through the use of algorithms, tend to exclude results deemed in contrast with the user’s “history” and preferences: the effect is to isolate people within their own “bubble” of information;³² and this, as we shall see later, has significant consequences on many processes, including that of innovation and, more specifically relevant for our purposes here, that of the formation of public opinion.

2.1. Law-making by the people: the limits of direct democracy

The digital age has made it much easier to resort to forms of consultation with the population, thus giving the illusion of being able to establish genuine “governments of the people.” The claim to involve citizens in more and more decisions, by means of electronic procedures, seems to be inspired by the same Jacobin ideals that were professed towards the end of the 18th century: it was in 1793 when Robespierre argued that the assembly of the people’s delegates should deliberate in the presence of the entire people, in a vast building open to at least twelve thousand spectators.³³

It is well known how these proclamations ended up. Yet, the greater ease of access to direct democracy, made possible by technology, can have positive effects. The important thing is that it does not replace other forms of democracy, which, even when in crisis, appear better equipped to examine and take complex decisions.

Indeed, Hans Kelsen’s warning is still valid, i.e. that, for the modern state, direct democracy, understood as the formation of the will of the state in the assembly of the people, is practically impossible, and the condemnation of parliamentarism is at the same time the condemnation of democracy.³⁴ However, it is clear that technological development and disintermediation have had a devastating impact on the equilibrium of the threefold articulation of political unity, namely the state, the parties, and the people.³⁵

Tools of direct democracy can also be useful, thanks to technology, in contexts where democratic forms of legitimation are lacking, or are less evident than in state systems. In international regimes, for instance, where global institutions have to adopt an increasing number of regulatory measures, such as guidelines, policies or standards, for example, the solution of directly involving the addressees of these rules, using participatory notice and comment mechanisms, is widely practiced. An em-

³¹ F. FOER, *World Without Mind. Why Google, Amazon, Facebook and Apple Threaten Our Future*, London, 2017, 67 ff.

³² E. PARISER, *Filter Bubble: How the New Personalised Web is Changing. What We Read and How We Think*, New York, 2012.

³³ M. ROBESPIERRE, *Discours sur le gouvernement représentatif, prononcé à la tribune de l’Assemblée nationale*, le 10 mai 1793. See also S. CASSESE, *Il popolo e i suoi rappresentanti*, with texts by Orlando, Spaventa, Sonnino, Giolitti, Croce, Rome, 2019.

³⁴ H. KELSEN, *Il problema del parlamentarismo (Das Problem des Parlamentarismus, 1925)*, transl. it., Torino, 2018, 77 ff., here 80.

³⁵ We take up here Carl Schmitt’s tripartition, ‘*Staat, Bewegung, Volk*’ (1933), in the reading provided by Giorgio Agamben (in the Introduction to C. SCHMITT, *Un giurista davanti a ses stesso. Saggi e interviste*, 2nd ed, transl., Vicenza, 2012, 1 ff.).

blematic case is the World Anti-Doping Code approved by the World Anti-Doping Agency (WADA) at the end of a lengthy procedure involving the online publication of several versions of the text and the possibility of submitting comments even by email.

Even in global regimes, however, ambiguities are not lacking. In fact, the very concept of disintermediation and the ‘myth’ of direct democracy can weaken the foundations of systems characterized by other forms of legitimacy, such as those built on expertise and technical-scientific competence. Excessive demand for popular legitimacy can harm ultra-state institutions. The *raison d’être* of these bodies rarely originates in representative requirements, but usually rests on the functional need to solve or otherwise deal with problems on a planetary scale.

Direct democracy is therefore an instrument better suited to local or neighborhood realities. Faced with the complexity of decisions that escape oversimplification, it shows all its inadequacy. In this respect, the case of Brexit is perhaps the most striking, because here the decision was taken using a referendum without considering the articulated range of implications and alternatives that its implementation would entail.³⁶

This is why the proposals to introduce popular legislative initiatives to be approved by referendum raise skepticism. How can the resolution of complex issues such as those typically dealt with in a legislative act be reduced to a binary choice (yes/no)? And how should parliament approach laws which have been approved “directly” by the people? Could it amend them or not?

A different situation is that of using technology and digital tools to facilitate the use of existing participatory institutions, such as, in Italy, abrogative referendums. In this case, the possibility of collecting signatures also by digital means was discussed for the 2022 referendums, but the Italian Privacy Authority (*Garante per la protezione dei dati personali*) expressed a negative opinion on the draft decree of the Prime Minister that was supposed to regulate the platform for the collection of voters’ signatures, implementing the legal provision introduced at the end of 2020. In particular, the Authority noted numerous problems with regard to data processing and the operation and security of the platform.³⁷

In conclusion, while technological development has undoubtedly favored the increased use of forms of direct democracy, it is important to emphasize three aspects.

The first aspect is one of context. There are several signs that point to a state of distress in contemporary democracies, even the oldest ones, such as the United Kingdom. Some scholars have even observed that the world has entered a period of “democratic recession”.³⁸ Indeed, the literature on the “death” and “end” of democracies is very rich.³⁹ Larry Diamond, for instance, has pointed out, also using data collected by Freedom House, that between 1974 and the end of 2014, 29% of the world’s

³⁶ F. FABBRINI (ed.), *The Law and Politics of Brexit*, Oxford, 2017.

³⁷ The opinion, delivered on 24 March 2022, is available at <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9760791>.

³⁸ L. DIAMOND, *Facing Up to the Democratic Recession*, in *Journal of Democracy*, 26, 1, 2015, 141, and F. FUKUYAMA, *Identity: The Demand for Dignity and the Politics of Resentment*, New York, 2018. See also S.P. HUNTINGTON, *The Third Wave. Democratization in the Late Twentieth Century*, Norma, 1991.

³⁹ S. LEVITSKY, D. ZIBLATT, *How Democracies Die*, above, and D. RUNCIMAN, *How Democracy Ends*, London, 2018; J. GOLDBERG, *Suicide of the West: How the Rebirth of Tribalism, Nationalism, and Socialism Is Destroying American Democracy*, New York, 2018.

entire democracies would have “collapsed”; and, in the first fifteen years of the 21st century, the rate of ‘failure’ (at 17.6%) was higher than that recorded in the previous fifteen years (at 12.7%). If we look at what has happened since 2000, there have been several reasons for this: a military *coup d’état* (as in Honduras, Mali or Thailand); electoral fraud (as in Burundi, Georgia, Kenya and Ukraine); widespread degeneration of executive power, including the violation of the rights of minorities and oppositions (as in the Philippines, Nicaragua, Turkey and Sri Lanka).⁴⁰ However, there are also scholars who contest this reading; while acknowledging the current difficult moment in which democracies find themselves, they point out that one cannot speak of a “democratic recession”, simply because the phase of expansion of democracies immediately after the end of the Cold War was somewhat overestimated.⁴¹

In this context, the spread of direct democracy mechanisms runs the risk of turning into a plebiscite-type instrument capable of reinforcing authoritarian and illiberal political systems. In other words, in the current historical conditions, it does not seem wise or prudent to ride the technological revolution to envisage improbable realizations of a direct democracy, with the people called upon to pronounce from home on highly complex decisions that require weeks, months and sometimes years of study and preparation. Societies, after all, are born because of a division of labor, based on skills that may require different levels of knowledge.

The second aspect is that direct democracy, in targeting representative and parliamentary democracy, seems to focus on the wrong target. In fact, technology can in the first place make it easier to develop forms of consultation in major administrative decisions, such as the location or construction of infrastructure. It would therefore be much more fruitful to downgrade the importance of direct democracy and popular legislative initiatives, and instead focus on so-called deliberative democracy. For example, structured participatory methods should be ensured, with institutions, means and procedures that can ensure the timely and effective involvement of stakeholders.

The spread of technology, therefore, instead of backing the Jacobin utopia of a popular legislature, can usefully support targeted instruments of direct democracy aimed at complementing – not replacing – representative democracy. Moreover, it can foster citizens’ involvement in administrative decisions through forms of deliberative democracy. In addition, it can ensure greater transparency of decision-making processes: the division of functions and tasks remains, but for the highest political one, technology could represent an instrument of ‘control’ by citizens of their delegates to that task.

The third aspect is that technology can also facilitate the involvement of citizens in the decisions of political parties, groups, or movements, even on very important issues. This is what has been attempted in Italy, for example, with the Five Star Movement’s Rousseau platform, which in September 2019 was also used to consult the movement’s members on the formation of a new government (with 80,000 people taking part in the vote).

Among the technological tools used to increase the involvement of administrators in public policy decisions is the adoption of some so-called gamification techniques. Examples of this are the use of rankings, or otherwise playful forms to improve the effectiveness of public authority action or determine certain allocative choices. Gamification basically presupposes the use of games to better de-

⁴⁰ L. DIAMOND, *Facing Up to the Democratic Recession*, above, 144 ff.

⁴¹ S. LEVITSKY, L. WAY, *The Myth of Democratic Recession*, in *Journal of Democracy*, 26, 1, 2015, 45.



fine public policies or to improve certain aspects of them. The adoption of gamification techniques – almost always by means of “apps” – in the definition and implementation of public policies, especially when combined with behavioral sciences, can ensure the effective involvement of the population and citizens in public decision-making processes.⁴² The case history is now rich and varied, covering many countries (the United States mainly, but also Australia, Iceland, Peru and Spain) and numerous international programmes or organizations (the World Food Programme, UNESCO, WHO, ILO and the EU, to name a few).

A different matter, however, is the dissemination of technology within parliaments and the use of digital tools for the conduct of business. This aspect was the subject of much debate during the 2020 pandemic, when there was a real risk that legislative assemblies would not be able to physically meet in presence due to the health emergency. The solutions were different, even with some innovative solutions, always considering the parliamentary regulations and constitutions of the different states: for example, in March 2020, the European Parliament met virtually, with remote voting; in Spain, online voting was allowed, while in the United Kingdom this formula was used for question times to government members. In general terms, beside the very etymology of the term, a parliament in which there is no real possibility of meeting, debating, and arguing does not seem to fully guarantee the fulfilment of one of the most important functions in a democracy, i.e. the legislative one.

2.2. Robot judges?

The use of algorithms by public authorities can in theory bring benefits to the decision-making process, for instance by eliminating subjective components that can also produce unbiased outcomes. The ethical and legal problems that arise, however, are obvious: what “arguments” does an algorithm use to justify its choice? How can one defend oneself against a decision constructed using such formulae? Who is ultimately responsible?⁴³

The increasing use of increasingly sophisticated algorithms primarily concerns two fundamental functions in the structure of the democratic state: the judicial function and the executive-administrative one.⁴⁴

In the first respect, the United States has long offered several examples of the application of predictive algorithms in the judiciary, the legitimacy of which has been questioned. Among the most famous precedents is the so-called ‘Compas case’, decided by the Supreme Court of Wisconsin. Compas (Correctional Offender Management Profile for Alternative Sanction) is a computer programme developed by a private company. It is an algorithmic system used in US courts for several decades to calculate the likelihood of recidivism of defendants or prisoners. It is a statistical processing of data collected by means of a questionnaire (with questions on various parameters, such as age, education, work, trial data, etc.).

⁴² G. SGUEO, *Games, Powers & Democracies*, Milan, 2018; Id., *The Design of Digital Democracy*, Cham, 2023.

⁴³ A. SIMONCINI, *L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Rivista di BioDiritto – BioLaw Journal*, 2019, 1, and Id., *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 2019, 1149. See also H.-W. MICKLITZ, O. POLLICINO, A. REICHMAN, A. SIMONCINI, G. SARTOR, AND G. DE GREGORIO, *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

⁴⁴ A. CARLEO (ed.), *La decisione robotica*, Bologna, 2019.



In the court case at hand, the defendant, who was stopped driving a car that had been used during a shooting, was given the maximum sentence. He then appealed the sentence, claiming a violation of ‘due process’, because the sentence was based on the calculation of an algorithmic system protected by copyright and unknown to him. After several instances, the Wisconsin Supreme Court recognized the legitimacy of the use of algorithms to calculate the risk of recidivism but reaffirmed that this calculation cannot be the sole basis for the judge’s decision.

Beyond the *Compas* affair, in which the plaintiff complained of being discriminated against by the algorithm, many argue that the use of algorithms, through an approach based on “constructing unbiased decision counterfactuals,” would reduce unequal treatment related to the gender or racial origin of the individuals involved.⁴⁵ However, it is clear that possible discrimination – on the basis of race, census, profession or educational level, for example – may arise at the moment when algorithmic parameters are defined and entered into the system. That is why the Council of Europe’s Commission on the Efficiency of Justice (CEPEJ) has adopted a special Ethics Charter on the use of Artificial Intelligence systems in legal proceedings.⁴⁶ And non-discrimination is one of the objectives of the Declaration on Ethics and Protection in Artificial Intelligence adopted by the International Conference of Data Protection and Privacy Commissioners in Brussels on 23 October 2018.

In any case, a sign of the skepticism that still accompanies the use of predictive tools in the judiciary comes from France. Here, law no. 2019-222, also dedicated to justice reform, passed in 2019, even punishes those who publish statistics on decisions or judges with up to five years’ imprisonment.⁴⁷ And, more generally, the use of automatic decision-making mechanisms by judges continues to raise many doubts.⁴⁸

2.3. Automated administrative decisions

As for the use of algorithms in administrative decisions, there are now numerous areas in which the process relies, to a greater or lesser extent, on such tools⁴⁹. It is no coincidence that, in Italy, the *Agenzia per l’Italia Digitale* published, in 2018, a White Paper on artificial intelligence at the service of the citizen.⁵⁰

If we consider Italy, the use of algorithms is now widespread, for example, to calculate the amount of public funding (this is the case of contributions from the National Fund for the Performing Arts),⁵¹ in

⁴⁵ J. KLEINBERG *et al*, *Human Decisions and Machine Predictions*, in *The Quarterly Journal of Economics*, 133(1), 1 February 2018, 241, cited by C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico europeo e comparato*, 2019, 101.

⁴⁶ <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

⁴⁷ https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33. On predictability in the legal sphere, A. CARLEO (ed.), *Calcolabilità giuridica*, Bologna, 2017.

⁴⁸ One can read the sharp reflections of M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, 3/2018, and in A. CARLEO (ed.), *La decisione robotica*, above, 63 ff.

⁴⁹ G. AVANZINI, *Decisioni amministrative e algoritmi informatici*, above.

⁵⁰ <https://www.aqid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2018/03/21/lintelligenza-artificiale-al-servizio-del-cittadino-sfide-opportunita>.

⁵¹ Tar Lazio, Rome, no. 7479/2016; Cons. Stato, no. 5035/2016



tender procedures (in electronic auctions or even for the automatic exclusion of bids)⁵² or to determine the evaluation of candidates for the assignment of seats (this is the well-known affair of the distribution of teachers in public schools). In all these cases – but there are also others, such as the automated penalties of the Highway Code or the automated Certified Declaration of the Start of Activity (the so-called Scia)⁵³ – there have been case law decisions that have helped to better identify the problems associated with the use of algorithms in administrative procedures.

The area that in Italy has so far offered the greatest elements of study and insight into the use of algorithms in administrative decisions and the related judicial review is that of public-school teachers and their distribution in different locations. It all stems from the fact that, as part of the recruitment procedures provided for in Law No. 107 of 2015, the Ministry of Education, University and Research had used an algorithm to ‘process’ the positions of the different teachers for the purposes of their allocation to the various locations. Some teachers filed an appeal complaining of an infringement of the right to defense. In the first instance, the Regional Administrative Court (TAR) of Lazio ruled in favor of the plaintiffs, considering that the use of computer mechanisms and systems to manage an administrative procedure was incompatible with the legal framework and the protection of the rights of the administrators.

The Council of State, however, intervening in 2019 on another case also concerning teacher assignment procedures, corrected the approach of the Lazio Regional Administrative Court, which had essentially rejected the use of algorithmic systems by the Ministry of Education, University and Research.⁵⁴ This decision represents an important landmark in the jurisprudential interpretation of the use of algorithms by public administrations. In particular, four features of the ‘algorithmic rule’ were identified:

1. the *legal-administrative nature*: although declined in mathematical form, the algorithmic rule possesses full legal and administrative value and, as such, is subject to the general principles of administrative activity, such as those of publicity and transparency, reasonableness, or proportionality;
2. the *absence of discretion*: the algorithmic rule cannot leave room for discretionary application (of which the computer is devoid), but must reasonably provide a defined solution for all possible cases, even the most improbable (and this makes it somewhat different from many general administrative rules); administrative discretion, if it certainly cannot be left to the software, is therefore to be found at the time of the elaboration of the digital instrument;
3. *it cannot take the place of the administration*: it must be the latter that performs an *ex ante* role of mediation and composition of interests, also by means of constant testing, updating and refinement of the algorithm (especially in the case of progressive and deep learning);

⁵² Tar Lazio, Rome, sec. *III-bis*, no. 5825/2019, no. 8902/2018 and no. 8312/2016; Cons. St., sec. VI, no. 5136/2017. Here the judges clarified that “the IT procedures applied to administrative procedures must be placed in a necessarily servant position with respect to the same, since it is inconceivable that, due to technical issues, the orderly conduct of relations between private parties and the Public Administration and between Public Administrations in their reciprocal relations should be hindered” (Author’s translation).

⁵³ A wide range of examples is in G. AVANZINI, *Decisioni amministrative e algoritmi informatici*, above.

⁵⁴ Cons. St., sec. VI, no. 2270/2019. On the notion of algorithm, see also Cons. St., sec. III, no. 7891/2021.

4. *judicial review*: the algorithmic rule must provide for the possibility of the judge to carry out, for the first time on a ‘human’ level, the evaluations and assessments made automatically; the robotized decision requires the judge to assess the correctness of the automated process in all its components. The arguments developed by the Italian Council of State with reference to the teachers’ case seem to strike a balance between the different interests and positions involved, in particular between the requirements of good performance of the public administration and the guarantees in favor of the citizen (transparency, access, duty to state reasons, right of defense).

Moreover, this is in line with what is happening in countries that have already adopted specific directives on automated decision-making. This is the case in Canada, where the Directive on Automated Decision-Making was issued in May 2019, directed at public administrations and in force as of 1 April 2020.⁵⁵ In addition to providing a useful set of definitions – such as, among others, those of artificial intelligence, source code and automated decision-making system – the directive aims to reduce the risks arising from the use of technologies and algorithms in decision-making processes. The requirements are therefore the impact assessment that must precede the use of any algorithmic system, transparency measures, motivation obligations, access to information (including source code, unless it falls under the exclusion hypotheses already established by the Access to Information Act for documents), quality standards (including the requirement for human intervention).

The issue of transparency is central in avoiding possible abuses resulting from the use of algorithms and the dissemination of automated decisions. For this reason, some administrations, such as the cities of Amsterdam and Helsinki, have set up registers in which the algorithms used by their offices are published. In particular, the registers make available to citizens the algorithm and AI systems used, the data employed, the logic of operation and the governance mechanisms.⁵⁶

In conclusion, the growing use of algorithms in state decision-making processes seems so far to have found a possible balance in ensuring, in any case, the protection of certain fundamental rights, also thanks to keeping some choices – and their reviewability – under the responsibility of the human being. The problem, however, is to understand how this balance can be guaranteed as the development of artificial intelligence and so-called machine learning will make it increasingly difficult to distinguish the different moments and stages. Above all, the gradual refinement of predictive algorithmic and learning systems leads to the merging of the support phase with the decision-making phase in the proper sense, postponing any disputes to the choice of parameters, criteria and instructions given to the ‘machine’. This, however, beyond the possible problems related to the intellectual property of the programme and the source code and their confidentiality, poses problems about the effective exercise of the right of defense. As has been pointed out, “the mere knowledge of the existence of an algorithm does not in itself produce any effect if one is not able to decipher its logic, that is, if one cannot understand *why* it puts together data in a *certain* way and thus reaches *certain* conclusions.”⁵⁷

⁵⁵ <https://tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

⁵⁶ The registers are here: for Amsterdam, <https://algoritmeregister.amsterdam.nl/en/ai-register/>; for Helsinki, <https://ai.hel.fi/en/ai-register/>.

⁵⁷ A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, above, 1184 (Author’s translation).



In this perspective, the attempts at regulation undertaken at supranational level on artificial intelligence (AI) are to be welcomed, not least to ensure coordination and uniformity between the various legal systems.⁵⁸ Among the initiatives taken, one should note, within the EU, the 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, of June 2021.⁵⁹

3. A surveillance state? *Privacy, walls and democracy*

New technologies, as we have seen, have a strong impact on the protection of fundamental rights, such as the right of defense or the right to privacy and protection of personal data. The risks of the use of automated mechanisms by public authorities are obvious, which is why the EU's General Data Protection Regulation (the so-called GDPR) stipulated that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."⁶⁰

To understand the dangers of abuse in the processing of personal data, it is sufficient to consider the increasingly widespread practice of 'profiling' of users, i.e., according to the definition offered by Article 4 of the GDPR, any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

In this respect, the solution of the so-called "informed consent", which is still adopted today through the request to accept the long list of terms and conditions concerning the processing of data by those who acquire them, does not seem satisfactory.⁶¹ This is not only because users almost never read or are able to understand the information they are asked to accept, but also because it is often very difficult to verify the actual use that is made of the data and profiling: this is exactly what happened in the well-known Cambridge Analytica case, where the data of tens of millions of Facebook users were used to convey information in order to influence the outcome of the 2016 US presidential election.

The basic problem is that the large network operators, and in particular the companies that manage the main social media, act and have set up their data collection and processing in terms of "surveillance".⁶² Confirmation of this attitude comes from the fines that have already been imposed on them by various authorities in various countries: in Italy, for example, Facebook was fined €10 million by the Competition and Market Authority for not having "adequately" and "immediately" informed users that their data was also being collected for commercial purposes; in Germany, in 2019, the Anti-

⁵⁸ M. Chinen (ed.), *The International Governance of Artificial Intelligence*, Cheltenham, 2023.

⁵⁹ Of particular interest is point 3.5 of the explanatory report, in which the relationship between IA and fundamental rights is highlighted (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=IT>). The text has been under negotiation between Parliament and Council since June 2023.

⁶⁰ Article 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. See also Articles 13(2)(f) and 14(2)(g) of the GDPR.

⁶¹ C. CASONATO, *Artificial intelligence and constitutional law: first considerations*, above; R. DEIBERT, *The Road to Digital Unfreedom: Three Painful Truths About Social Media*, in *Journal of Democracy*, 30, 1, 2019, 25-39.

⁶² R. DEIBERT, *The Road to Digital Unfreedom: Three Painful Truths About Social Media*, supra, 26 ff.

trust Authority charged the same company with an abuse of its dominant position, again with regard to the way in which data was acquired.⁶³ This is also why, in March 2019, Facebook published the document “A Privacy-Focused Vision for Social Networking”,⁶⁴ aimed at closing, at least in its intentions, many of the loopholes that emerged in these and other proceedings.

At other times, the protection of personal data can also be an important tool to limit the potential negative effects of the development of systems based on AI like ChatGPT. This is what happened in Italy, when in March 2023 the Privacy Authority (*Garante per la protezione dei dati personali*) suspended the activity of ChatGPT for unlawful collection of personal data and absence of systems to verify the age of minors.⁶⁵

There is, in essence, the crucial question of the value now acquired by data. This value increases in direct proportion with the growth of their volume, their variety and the velocity with which they are acquired and processed: these are the so-called ‘Vs’ that identify big data, to which are added others, such as veracity, validity, and visualization.⁶⁶ As some have already pointed out, the economy of the future will probably see the possibility for some subjects to ‘sell’ their data, something they cannot do at present, in the sense that their data are already owned by other subjects who make use of them, even commercially, because the actual owners have given their consent without having actual or full knowledge of it.

The protection of personal data thus appears to be the most immediate of the needs brought about by the technological revolution. But, as we have seen, it is not the only fundamental right whose protection may be jeopardized by the increasingly widespread use of technology by public authorities.

First of all, there are the risks, highlighted earlier, linked to the use of algorithms in decision-making processes. This is where the most basic guarantees of citizens, conquered over the centuries, come into play in the face of possible excesses of power on the part of public administrations: duty to give reasons, transparency, access to information, right of defense.

Then there is the protection of the freedom of expression.⁶⁷ This may be restricted whenever any form of ‘moderation’ of content is implemented by network or social media operators. Such moderation, however, is necessary both to ensure the protection of other fundamental rights, and to prevent or combat crimes, and also, as we shall see later, to allow a ‘correct’ formation process of public opinion. These aspects concern more directly, however, the problem of the relationship between technology and information, as well as, in broader terms, that between democracy and truth.

The technological revolution then produces ambiguous effects on borders and on the very notion of territory, especially with regard to the last great limitation that today holds back the realization of a global space: the free movement of persons. In fact, the new technologies strengthen the States that

⁶³ M. DELMASTRO, A. NICITA, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019, 45 ff.

⁶⁴ <https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/>.

⁶⁵ <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847>.

⁶⁶ D.H. HOLMES, *Big Data. A Very Short Introduction*, Oxford, 2017, 15 ff., and M. DELMASTRO, A. NICITA, *Big Data, above*, 25 ff. Also L. FLORIDI, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford, 2023, 67 ff., and S. MANNONI, G. STAZI, *Sovereignty.com. Potere pubblico e private ai tempi del cyberspazio*, Naples, 2021, 241.

⁶⁷ G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI, *Parole e potere. Libertà d’espressione, hate speech e fake news*, Milan, 2017.

intend to guard and defend their borders, countering migratory phenomena: passports with biometric data, drones flying over the borders, algorithms to monitor entry flows, satellite controls, are just a few examples. Moreover, the ‘dark side’ of artificial intelligence shows a massive use of these technologies for security, public order and intelligence purposes.⁶⁸

Data show that the number of people who need a passport and a visa to move from one country to another is very high. To get an idea of this, we can look at the so-called Passport Index, which measures the ‘strength’ of a passport according to the number of countries into which it allows entry without a visa or with the possibility of obtaining a visa on arrival (and thus not before departure).⁶⁹ According to this index, in 2023 the United Arab Emirates ranks first, with 180 territories – the system registers 227 destinations – followed with 176 by Austria, Germany, Finland, France, Italy, Luxembourg, the Netherlands, Spain, Sweden and Switzerland. For half of the countries, a passport alone allows visa-free travel in just 90 territories. In last place is Afghanistan, whose passport allows entry, without a visa or with a visa obtained on arrival, to just 6 destinations.

But it was not always so. At the beginning of the 20th century, to give an example, barely 10% of travelers entering the British Isles had to pass a border control, which at the time consisted simply of stating orally where one intended to stay: in 1909, 422,000 people were “checked” and none were turned back, which did not prevent public opinion from strongly criticizing these measures as illiberal and “unworthy of a civilized country”.⁷⁰

At the same time, technology could in the future favor cheaper modes of travel and at least reduce the cost of transporting people in person: this would represent a further pressure factor towards the borders of those states that block the entry of foreigners. The question then becomes whether an easier crossing of borders could lead to a reconsideration of the very idea of territory which, even today, is one of the constituent elements of the notion of statehood.

The creation and expansion of the Internet and other means of information and communication have contributed decisively to removing one of the three so-called constraints to globalization, namely that of the circulation of ideas.⁷¹ According to this well-known reconstruction, the development of information and communication technologies can be traced back to the “second unbundling” of globalization, after the one brought about by the industrial revolution with the invention of the steam engine (which led to overcoming the constraint of the circulation of things, as well as improving that of people). The multiplier effect of the digital revolution, albeit in a mediated way, has also unleashed the potential of previous technological advances by making them within the reach of many. The third constraint, which has not yet been broken for the majority of the world’s population, is that of the movement of people.

One can understand, therefore, why so-called sovereigntist political positions insist so much on the issues of countering immigration and closing borders and ports, pursuing the idea of a “coastguard

⁶⁸ K. CRAWFORD, *Atlas of Ai: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale, 2022.

⁶⁹ <https://www.passportindex.org/byRank.php>.

⁷⁰ G. SCIORTINO, *Rebus immigrazione*, Bologna, 2017, 20 ff. (Author’s translation).

⁷¹ R. BALDWIN, *The Great Convergence. Information Technology and the New Globalization*, Harvard, Cambridge, 2016, 85 ff.

state” or “customs state”. The Internet is borderless, but in the real world, barriers and expulsions are increasing.⁷²

In his mapping of walls in history and around the world, Tim Marshall, for 30 years correspondent for the BBC and Sky News, describes, for example, when in 2014 the inhabitants of Encarnación, a small town in Paraguay, were separated from their Argentine neighbors in Posadas by a reinforced concrete wall more than 4 meters high, erected on the Argentine side of the Paraná river for about 1 km: the purpose was to contain the flow of possible Bolivian migrants who might arrive in Argentina via Paraguay.⁷³

Similarly, in her book on ‘Walled States’, the political philosopher Wendy Brown already in 2010 gave an account of the ever-increasing number of walls that are being erected in the world: not only the best-known walls, such as the one between the United States and Mexico and the Israeli one, but also those between South Africa and Zimbabwe, between Saudi Arabia and its neighboring countries, between India and Pakistan, between Uzbekistan and Afghanistan, or even in Botswana, Thailand, Malaysia, China, Egypt, Brunei.⁷⁴

With the increase of walls and fences, the illusion is pursued that, by strengthening the constraint that still holds back globalization more than any other, states can alone defend their sovereignty and do without others. But, as has been pointed out by Sabino Cassese, another paradox is produced here: the sovereigntist states demand that international institutions support them in imposing their decisions, thus they themselves admit and acknowledge that, without the help of other powers, even ultra-state powers, they cannot achieve the goals they have set for themselves.⁷⁵

The overcoming of borders and the challenges to the sovereignty of states not only concern the globalization of people, things and ideas, but has now also involved one of the most traditional and ancient powers of public power and the state, that of issuing money. The reference here is not to the birth of a common currency among several nations, as was the case with the Euro in Europe, but to the creation of electronic currencies or crypto currencies.

With the development of blockchains and the spread of bitcoins, the use of currencies with no ties to states is also on the horizon, going beyond what has already happened with the euro, “*une monnaie sans État pour le XXIe siècle*”.⁷⁶ Blockchains are “private or public (authorized, the former) networks made up of nodes (the participants’ servers) that contain blocks of information organized in a database. Any activity – a transaction, for example – is only effective if it is approved by all the blocks in the network, which therefore record it, keep it in memory, automatically verify (mining) its legitimacy, certifying that it comes from an authorized party”.⁷⁷

The operation of these networks would guarantee security, transparency, immutability (of the data), confidentiality and limited costs (but the high energy consumption for maintaining the servers must

⁷² This is pointed out by S. SASSEN, *Expulsions: Brutality and Complexity in the Global Economy*, Cambridge: MA, 2014.

⁷³ T. MARSHALL, *Divided: Why We’re Living in an Age of Walls*, London, 2018.

⁷⁴ W. BROWN, *Walled States, Waning Sovereignty*, New York, 2010.

⁷⁵ This is repeatedly emphasised by S. CASSESE, *La svolta. Dialogues on changing politics*, Bologna, 2019.

⁷⁶ T. PIKETTY, *Le Capital au XXIe siècle*, Paris, 2014, 1015.

⁷⁷ F. BASSAN, *Potere dell’algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi*, Soveria Mannelli, 2019, 46 ff. (Author’s translation).

be considered). The pros and cons of using these systems, precisely about the new electronic currencies, have also been examined by the European Parliament, in its Resolution on virtual currencies of 26 May 2016 (2016/2007(INI)) and in its Resolution on distributed ledger and blockchain technologies: building trust through disintermediation of 3 October 2018 (2017/2772(RSP)).

In addition to the so-called cryptocurrencies, the Libra project devised by Facebook to introduce its own electronic currency, which could potentially affect more than 2 billion people, was perhaps the clearest sign of the companies' attempt to completely overcome the link between the state, sovereignty and the issuing of currency.⁷⁸ Not surprisingly, the reaction of states to this project was very negative.⁷⁹ On the other hand, Libra presented itself as a stable coin, because it was linked, in turn, to a collection of currencies and other assets placed to guarantee its non-volatility. Unlike the 'pure' bitcoins, therefore, Libra seemed to go beyond the simple will of a large private multinational company to compete with the state, highlighting further ambiguities and contradictions in the relationship between technologies and public powers: on the one hand, in fact, it escapes statehood and the monopoly of minting money; on the other hand, however, it anchors the currency to other currencies and real assets, and Facebook had created an association – Libra – based in Switzerland, thus exploiting the guarantees of statehood itself. The Libra project, as anticipated, came to a halt in early 2022. But the spread of cryptocurrencies has not stopped: in September 2021, for instance, the state of El Salvador adopted *bitcoin* as legal tender in its territory; in April 2022, this choice was also made by the Central African Republic.

Finally, the relationship between borders and technological development shows a further paradox: the more the world's communications and connections increase, the more physical means are needed to do so. Of these, the most important is still the underwater cables connecting different continents. Figures show that around 95 per cent of the world's communications pass underwater, totaling 378 cables and over 1.2 million km. This is why there is now a real geopolitical battle between the United States and China for control of underwater cables.⁸⁰

4. Technology and (dis)information

There is, finally, a further area to be analyzed and which requires special investigation, namely that of the relationship between technology and information, between democracy and truth.⁸¹

The issue of *fake news* and disinformation is probably the most difficult challenge for contemporary democracies. On the other hand, Michel Foucault pointed out well a few decades ago that the forms and ways in which truth is represented and communicated play a crucial role for any form of government and its "alethurgic" function: "*alèthurgie*" is "*une manifestation de vérité*" understood as "*l'ensemble des procédés possibles, verbaux ou non, par lesquels on amène au jour ce qui est posé*

⁷⁸ T. ADRIAN, T. MANCINI-GRIFFOLI, *The Rise of Digital Money*, International Monetary Fund, 2019; see also the annual report of the *Bank for International Settlements* (2019), with a section on "Big Tech in Finance: Opportunities and Risks", and subsequent reports, which deal with the topic of *digital currencies*.

⁷⁹ <https://www.ft.com/content/0c5c4012-9100-11e9-b7ea-60e35ef678d2>.

⁸⁰ A. ARESU, *Gli imperi dei cavi sottomarini*, in *Limes*, 2019, 61 ff.

⁸¹ G. RIVA, *Fake news*, Bologna, 2018, and A. NICITA, *Il mercato delle verità. How disinformation threatens democracy*, above.

*comme vrai par opposition au faux, au caché, à l'indicible, à l'imprévisible, à l'oubli, et dire qu'il n'y pas d'exercice du pouvoir sans quelque chose comme une aléthurgie".*⁸²

The risks to democracy from disinformation have always been noted, especially in the vicinity of 'rupture' events, as was the case with the two world wars. We can mention these three passages, by Stefan Zweig, Ernst Cassirer, and Hannah Arendt respectively, which are still highly topical today: "*Meinung ist Masse, Überzeugung der Mensch. Und das Tragische der Zeit darum in einem Satz: die Meinungen haben über die Überzeugungen gesiegt. Das Gerede über das Gewissen. Überall*".⁸³

The politician becomes a sort of public fortuneteller. Prophecy is an essential element in the new technique of rulership. The most improbable or even impossible promises are made; the millennium is predicted over and over again.⁸⁴

In an ever-changing, incomprehensible world the masses had reached the point where they would, at the same time, believe everything and nothing, think that everything was possible and that nothing was true.⁸⁵

Thus, the vital links between democracy and the formation of public opinion have long been known: one need only read Lippmann's 'classic' study from the early 1920s or Herman and Chomsky's analysis of the political economy of the mass media – the "Manufacturing Consent" – some six decades later.⁸⁶ After all, influencing public opinion erodes the very essence of the legislative function, as Dicey already observed at the beginning of the 20th century in reconstructing the relationship between democracy and legislation.⁸⁷

In the 21st century, the incredible development of social networks has given every individual the opportunity to say anything: this 'gift' has also been relentlessly used for wrong purposes, including incitement to hatred and violence, disinformation, and interference in electoral competitions.

⁸² M. FOUCAULT, *Du gouvernement des vivants. Cours au Collège de France (1979-1980)*, Paris, 2012, 8. In English: "aléthourgia, alethurgy, from aléthourgēs, we could call "alethurgy" the manifestation of truth as the set of possible verbal or non-verbal procedures by which one brings to light what is laid down as true as opposed to false, hidden, inexpressible, unforeseeable, or forgotten, and say that there is no exercise of power without something like an alethurgy." (M. FOUCAULT, *On The Government of the Living (Michel Foucault, Lectures at the Collège de France)*, London, 2012, 7). See also P. HÄBERLE, *Wahrheitsprobleme im Verfassungsstaat*, Baden-Baden, 1995, J. NIDA-RÜMELIN, *Demokratie und Wahrheit*, München, 2006; S. ROSENFELD, *Democracy and Truth. A Short History*, Philadelphia, 2019, as well as H. ARENDT, *Die Lüge in der Politik. Überlegungen zu den Pentagon-Papieren (1971)*, available at <https://www.humanistische-union.de/publikationen/vorqaenge/167-vorqaenge/publikation/die-luege-in-der-politik/>.

⁸³ S. ZWEIG, *Opportunismus, der Weltfeind*, in *Das Forum*, 3, 1, 1918-1919 (Author's translation: "Opinion is mass. Conviction is man. And the tragedy of the present age, in one sentence, is this: opinion has triumphed over conviction. Chatter over knowledge. Everywhere.").

⁸⁴ E. CASSIRER, *The Myth of the State (1945)*, in Id., *Ernst Cassirer, Gesammelte Werke. Hamburger Ausgabe Book 25*, Hamburg, 2007, 284.

⁸⁵ H. ARENDT, *The Origins of Totalitarianism (1951)*, New York, 2017, 499.

⁸⁶ W. LIPPMANN, *Public Opinion*, New York, 1922; E. HERMAN, N. CHOMSKY, *Manufacturing Consent. The Political Economy of the Mass Media (1988)*, London, 2008. The point is well made by P. HÄBERLE, *Wahrheitsprobleme im Verfassungsstaat*, above, 93.

⁸⁷ A.V. DICEY, *Lectures on the Relation Between Law and Public Opinion in England During the Nineteenth Century (1905)*, London, 2017; see also J. HABERMAS, *Strukturwandel der Öffentlichkeit (1990)*, Frankfurt am Main, 2021 (on Dicey and the concept of 'public opinion', 348).

Meta, Google, and other large companies are already attempting to counter the scourge of “disinformation,”⁸⁸ especially during election periods.⁸⁹ The results of these efforts were visible for all to see during the campaign for the US presidential elections in 2020. Furthermore, in November 2019, Facebook set up an Oversight Board, a body consisting of up to 40 members chosen from experts in the field of content moderation and freedom of expression. The purpose of the Facebook Oversight Board is “to promote free expression by making principled, independent decisions regarding content on Facebook and Instagram and by issuing recommendations on the relevant Facebook Company Content Policy”.⁹⁰ From its inception to August 2023, the Board has published 46 decisions, including one on the Trump case (where it deemed the indefinite account suspension disproportionate): of these, most have concerned issues relating to hate speech, violence, discrimination, and security; very limited, therefore, have been cases of misinformation.

But is this enough to counter misinformation?⁹¹

In the above-mentioned article published in the ‘Washington Post’ in 2019, Mark Zuckerberg referred generically to the need to ensure the integrity of elections but did not include fake news among the so-called harmful contents. It should be remembered, moreover, that under the now well-known Section 230 of the US Communications Decency Act, platforms – like providers – are not treated like publishers or newspapers, for which there is a liability regime for published content: a clause that has provided substantial immunity to large social networks, but whose scope has been gradually eroded, especially in the European Union.

The spread of fake news in the political sphere probably found its peak, as seen, in the election campaign for the election of the President of the United States in 2020, when on several occasions social networks had to intervene with warnings or to remove untruthful posts spread by the candidates, in particular by then-President Donald Trump.

Moreover, the phenomenon of disinformation, multiplied by new technologies, triggers processes of falsification deliberately aimed not only at creating disorder, but even at replacing one order with another; the mediaeval paradigm of falsification, aimed at “reconfirming belief in something” and “sustaining an order” is thus completely overturned.⁹²

On the other hand, the rate of false news production has now reached alarming levels. In the United States, for example, the ‘Washington Post’ showed that President Trump produced between 6 and 7

⁸⁸ See *Information Operations On Facebook* (2017), <https://fbnewsroom.us.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>.

⁸⁹ N. PERSILY, *The 2016 U.S. Election: Can Democracy Survive the Internet?*, in *Journal of Democracy*, 2017, 28, 63; A. EYRIÈS, *La twit-politique: l'élection présidentielle française de 2017 sur les réseaux sociaux numériques*, in *La datacratie*, above, 87 ff.

⁹⁰ <https://www.oversightboard.com>.

⁹¹ M. HAIM, A. GRAEFE, H.-B. BROSIUS, *Burst of the Filter Bubble?*, in *Digital Journalism*, 6, 2018, 330; M. CARLSON, *Facebook in the News: Social Media, Journalism, and Public Responsibility Following the 2016 Trending Topics Controversy*, *ibid.*, 4 ff.; and J. WALLACE, *Modelling Contemporary Gatekeeping*, *ibid.*, 274; F. PASQUALE, *The Black Box Society*, cit, 59; K. KOWALIK-BAN' CZYK, O. POLLICINO, *Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information*, in *German Law Journal*, 17, 2016, 315.

⁹² U. ECO, *La falsificazione nel Medioevo* (1986), in *Id.*, *Dall'albero al labirinto. Studi storici sul segno e l'interpretazione*, Milan, 2017, 259, here 288 ff. (Author's translation).

Law
 &
 News

false claims per day in 2018.⁹³ Which is not surprising, considering that the Trump presidency itself began with the controversy over the actual number of people present at his inauguration speech.⁹⁴ It is no coincidence that in 2016, right after the Brexit referendum and Trump's election, the Oxford Dictionary proclaimed 'post-truth' as the word of the year, given its massive use: a term referring to "circumstances in which objective facts are less influential in shaping public opinion than appeals to personal emotions and beliefs".⁹⁵

In the UK, the 2019 Disinformation and 'Fake News' Final Report produced by the UK Parliament highlighted interference, including from abroad, directed at producing false information on the web and social media in relation to Brexit.⁹⁶ Again in the UK, while 90% of the population trusts the data provided by the Office for National Statistics, only 26% believe the UK government uses or reports it correctly.⁹⁷ EU data also tells us that 83% of people think disinformation is a threat to democracy, 63% of young Europeans encounter fake news more than once a week, 51% of Europeans believe they have been exposed to disinformation online.⁹⁸

The reasons why the Internet and social media disproportionately amplify the speed and extent of the spread of fake news are obvious. The ease of access, the 'emotional' dynamics of social networks, the phenomenon of the so-called echo chamber (whereby a user will tend to consider 'true' information consistent with his or her own beliefs), the effectiveness of the 'dominant' algorithms of the major companies (which increase the display of a post in relation to the number of 'likes' or 'retweets') are some of the reasons that exponentially accentuate the effects produced by any false information put on the net.⁹⁹

The 2020 pandemic has further highlighted the risks of misinformation, but also the need for states and public authorities in general to perform the 'aleurgical' function of communicating information correctly. The rate of conflict between those in favor and those against vaccines was unfortunately very high, but this was also due to an ineffective communication strategy on the part of governments, which was also conditioned by the uncertainty arising from an unprecedented situation. This was not helped by the initial context which, as confirmed by the data collected in the UK, was one of general lack of confidence in the reliability and accuracy of information provided by governments. Within this framework, disinformation, fueled by a climate of ideological confrontation and an underlying distrust of institutions, found fertile ground.

⁹³ L. DIAMOND, *Ill Winds. Saving Democracy From Russian Rage, Chinese Ambition, And American Complacency*, New York, 2019, 82. See THE WASHINGTON POST FACT CHECKER STAFF, *Donald Trump and His Assault on Truth: The President's Falsehoods, Misleading Claims*, New York, 2020.

⁹⁴ W. DAVIES, *Nervous States. How Feelings Took Over the World*, London, 2018, 1.

⁹⁵ M. ADINOLFI, *Hanno tutti ragione? Post-verità, Fake News, Big Data e Democrazia*, Rome, 2019 (Author's translation). See also M. FERRARIS, *Postverità e altri enigmi*, Bologna, 2017.

⁹⁶ The report, prepared by the *Digital, Culture, Media and Sport Committee* of the *House of Commons*, can be found here: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1791/1791.pdf>.

⁹⁷ W. DAVIES, *Nervous States*, above, 63, quoting an article from *The Independent* of 27 February 2017.

⁹⁸ https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan/strengthened-eu-code-practice-disinformation_it.

⁹⁹ G. PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI, *Parole e potere*, above.

It then becomes increasingly urgent to consider what options are available to stem the spread of these phenomena and counter the “toxic role of social media”.¹⁰⁰ In the short term, a mixed approach can be adopted that brings together all the different possible alternatives, including debunking and the creation of reliable sites dedicated to certain public events, such as elections. States and large private companies should work together to create official platforms for fact-checking and debunking fake news. It is clear how sensitive this aspect is because it evokes serious risks for the freedom of expression and may foreshadow the advent of new forms of censorship. The technical remedies adopted by companies for the moderation of content on social networks are constantly evolving:¹⁰¹ but should states leave it to Facebook or other private entities alone to counter fake news or guarantee the integrity of elections?

The provision of criminal sanctions, on the other hand, seems a less viable solution, for several reasons, such as the difficulty of identifying the real perpetrator of the hypothetical crime and the real nature of fake news. Therefore, the best practice solutions and awareness-raising campaigns that the European Union has experimented with to counter fake news,¹⁰² such as the “EU vs. Disinfo” initiative, which is essentially based on regular debunking through a ‘Disinformation Review’, seem more effective.¹⁰³ Furthermore, in June 2022, the new Strengthened Code of Practice on Disinformation was published by the European Commission, an update of the 2018 Code of Practice: among the strengths are activities aimed at empowering users, the scientific community and communities engaged in fact-checking.¹⁰⁴ One understands, then, the reasons that led some scholars to identify a form of “digital constitutionalism” promoted by the European Union, also in order to counter the dominance of platforms.¹⁰⁵

Information and communication play an essential role in democracy and there are obviously different types: between individuals, from one individual to a multitude, from many to many. It is generally the first and third types of information and communication that generate problems of control, privacy, security. Moreover, if states do not have the so-called big data, there will be enormous difficulties in constructing appropriate forms of participation.¹⁰⁶ Global law can therefore offer useful tools, to be verified together with the States. But this is not without problems, as the case of China shows, which still strictly controls the use of the Internet in its territory and has a massive surveillance pro-

¹⁰⁰ P. BARDHAN, *A World of Insecurity. Democratic Disenchantment in Rich and Poor Countries*, Cambridge, 2022, 31. See also Z. GERSHBERG, S. ILLING, *The Paradox of Democracy. Free Speech, Open Media, and Perilous Persuasion*, Chicago, 2022.

¹⁰¹ S. QUINTARELLI, *Content Moderation: i rimedi tecnici*, in G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI, *Parole e potere*, above.

¹⁰² A. ALEMANNI, *Editorial: How to Counter Fake News? A Taxonomy of Anti-fake News Approaches*, in *European Journal of Risk Regulation*, 1, 2018.

¹⁰³ <https://euvsdisinfo.eu>.

¹⁰⁴ <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.

¹⁰⁵ G. DI GREGORIO, *The rise of digital constitutionalism in the European Union*, in *19 International Journal of Constitutional Law*, 2021, 41.

¹⁰⁶ The ‘dark side’ of so-called *big data* was already highlighted by V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, London, 2013, 149 ff. See also C. DEVINS *et al.*, *The Law and Big Data*, in *Cornell J. L. & Pub. Pol’y*, 27, 2017, 357; H. KRAUSE HANSEN, T. PORTER, *What Does Big Data Do in Global Governance?*, in *Global Governance*, 23, 2017, 31; A. ALEMANNI, *Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many*, in *EJRR*, 9, 2018, 183.

gramme using technological tools:¹⁰⁷ the Chinese government spends “an estimated \$6.6 billion every year just on monitoring and censoring online content.”¹⁰⁸

These instruments may not only act at the regulatory or procedural level, but also at the organizational level: for instance, by creating an *ad hoc* international body¹⁰⁹, or by recognizing that the global corporations that govern the network operate in a *de facto* monopoly condition that makes them comparable to global public administrations, so as to require specific forms of control.¹¹⁰

In the medium and long term, there could be several policies to be adopted in order to overcome these “Democracy breaks” and for “Redirecting technology”, such as those related to market incentives for redirection, breaking up big tech, tax reform, privacy protection and data ownership, to name but a few.¹¹¹ Amongst different solutions, it remains crucial to invest in education, enabling children and adults to better understand the different levels and degrees of reading texts and to go beyond the immediate and often superficial information acquired through a Facebook post or a video on Tik-Tok. Recent studies have, moreover, shown that it is schooling that has now become the new “social discriminator, both at individual and community level, and that the economic fate of both American and European cities depends on the number of graduates”.¹¹² It is education that really makes democracy possible,¹¹³ and “everything that promotes cultural development also works against war”: this is how Sigmund Freud, in 1933, ended his reply to Albert Einstein who had asked him why war was necessary.¹¹⁴

The point is that it takes time to consolidate a democracy. Even in the United States, in relation to which many now denounce a state of democratic crisis, it took centuries. This is well described by Larry Diamond, who every year asks his students “When did the United States become a democracy?”. The answers range from 1776, with the Declaration of Independence, to 1789, with the approval of the Constitution, to 1865, with the abolition of slavery, and 1920, with the recognition of women’s right to vote. But the correct answer is 1965, when the *Voting Rights Act* finally put an end to racial discrimination in the Southern States: it was not until 1968 that “free and fair” presidential elections were held in the United States for the first time.¹¹⁵

¹⁰⁷ X. QIANG, *The Road to Digital Unfreedom: President Xi’s Surveillance State*, in *Journal of Democracy*, 30, 1, 2019, 53-67.

¹⁰⁸ D. ACEMOGLU, S. JOHNSON, *Power and Progress*, above, 340.

¹⁰⁹ Similarly to what could be done in the field of ‘cybersecurity’: see M. FINNEMORE, D.B. HOLLIS, *Constructing Norms For Global Cybersecurity*, in *AJIL*, 110, 2016, 425; K. MACĀK, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*, in *Leiden Journal of International Law*, 30, 2017, 877.

¹¹⁰ F. FOER, *World Without Mind*, above, refers to these societies as “monopolists of mind” (9 ff.) and “knowledge monopolists” (82 ff.).

¹¹¹ D. ACEMOGLU, S. JOHNSON, *Power and Progress*, above, 339 ff. and 383 ff.

¹¹² D. DE MASI, *Il lavoro nel XXI secolo*, Turin, 2018, recalling E. MORETTI, *La nuova geografia del lavoro*, Milan, 2012 (Author’s translation).

¹¹³ R. DWORKIN, *Is Democracy Possible Here? Principles for a New Political Debate*, Princeton, 2006, 147 ff. The topic is also treated by F. FUKUYAMA, *The End of History and the Last Man*, above, 109 ff.; and M. NUSSBAUM, *Not for Profit: Why Democracy Needs the Humanities*, Princeton, rev. edition, 2016, 27 ff.

¹¹⁴ S. FREUD, *Why War? Freud’s letter to Einstein: and other minor works*, United States, 35.

¹¹⁵ L. DIAMOND, *Ill Winds. Saving Democracy From Russian Rage, Chinese Ambition, And American Complacency*, supra, 17 ff.

5. What future for the digital state?

States are now surveyed and assessed according to the most diverse indicators and criteria. Statistical studies measuring states are thus numerous and examine almost every aspect, such as economic competitiveness,¹¹⁶ credit rating,¹¹⁷ the rate of democracy,¹¹⁸ or the level of 'statehood' itself.¹¹⁹ Between 2020 and 2022, unfortunately, states also entered the World Health Organization (WHO) measurements with regard to the number of people infected by COVID-19.¹²⁰

But how is the state really doing today?

There is often talk of its crisis, but also of its rebirth. In fact, although the idea of an end of the state or of a 'devalued' ('*dévalorisé*')¹²¹ state goes back a long way, several signs show that the concept of the state still enjoys good health today. In this respect, the pandemic crisis has further confirmed the dominant position of the state as the political community par excellence, with regard to both the protection of the health of its citizens and the (contested) control over the ways and forms of exercising fundamental freedoms.

It is therefore possible to say that today it is not the concept of the state that is in crisis, but rather the idea of a 'democratic' state, built on the separation of powers, that has been established from the late 18th century onwards. An idea of state in which the notion of sovereignty is closely linked to the maintenance of democracy.

At the same time, the paradox of the need to have other states in order to recognize a state is flanked by what Norberto Bobbio called the paradox "of all times", because states "can all become democratic only in a democratized international society. But a democratized international society presupposes that all states are democratic."¹²²

And it is precisely the initiatives from 'above' aimed at promoting democracy that confirm how central the idea of the state still remains in international law and relations. Global institutions are committed to supporting states, even to the point of measuring their statehood rate: this is the case, for example, of the Fragile State Index, the result of a series of indicators adopted by the Fund for Peace to assess, for each state, aspects such as the effective control of territory or the effective monopoly of the legitimate use of force, the possible loss of authority, the capacity or not to provide public services or even the capacity or not to interact with other states at an international level.¹²³

¹¹⁶ Global Competitiveness Report, as part of the World Economic Forum (<http://reports.weforum.org/global-competitiveness-reports/>).

¹¹⁷ The reference is to credit ratings by international agencies such as Standard & Poor's, Fitch and Moody's.

¹¹⁸ United Nations Democracy Fund (<https://www.un.org/democracyfund/>).

¹¹⁹ <https://fragilestatesindex.org>.

¹²⁰ <https://covid19.who.int>.

¹²¹ Thus R. ARON, *Paix et guerre entre les nations*, Paris, 1962, 392, with reference to nation-states.

¹²² N. BOBBIO, *La democrazia dei moderni paragonata a quella degli antichi (e a quella dei posteri)* (1987), in *Id.*, *Etica e politica. Scritti di impegno civile*, Milan, 2009, 1108 ff., at 1127 (Author's translation).

¹²³ See <http://fundforpeace.org/fsi/>.

Similarly, the focus on so-called state failure – and on so-called failed states –¹²⁴ highlights other paradoxes, linked to the use of global indicators. On the one hand, the various indices and rankings maintain the state – and states – as the ‘center of gravity’ of the world, to the point of also monitoring its state of health.¹²⁵ On the other hand, however, certain measurements – think of credit ratings – can have the effect of severely weakening state sovereignty, sometimes accelerating those processes of ‘failure’ that other international initiatives, on the other hand, aim to avert. And it is evident how much technological innovations can today accentuate and accelerate all these processes. So, can the development of communications and information that exploded in the 1990s with the end of the Cold War, and is still ongoing, really change the (modern) state and lead to a review of its constituent elements?

There are many different areas in which technology has already influenced or is influencing the life of public institutions. The limits of direct democracy, the use of algorithms in decision-making processes, the protection of fundamental rights, the border crisis and the relationship between technology and information have been examined above. To conclude these reflections, it is useful to dwell on two further challenges that await the state in the digital era: the relationship between states and large network multinationals, such as Meta and Google, with reference to the so-called big data; the relationship between the technological revolution and language, with regard to the process of forming and consolidating institutions.

5.1. The fate of big data: private v. public

The majority of personal data and information in the world today is acquired, stored and managed by private companies that need this information to make a profit, through advertisements or other forms of revenue. The above-mentioned Cambridge Analytica scandal highlighted the risks that a misuse of this information can cause, in that case even affecting the electoral competition of the world’s greatest power.

More generally, social networks have now become an information medium in their own right, which makes the phenomenon of disinformation systematically produced by political movements or governments even more serious: in the United States, for example, already in 2017 more than 60 per cent of Americans accessed news through social platforms, and more than a third of traffic to information sites went through Google.¹²⁶ It should never be forgotten, in fact, that, as Italo Calvino wrote in the late 1970s, “a democracy lives if the word is operative, that is, if criticism, denunciation, argumentation, the demand for truth do not pass without leaving a mark. And it is only in this climate that the just word is not confused with the unjust or slanderous or empty word”: and “the responsibility to say and to repeat what needs to be said grows with the hardening of the times.”¹²⁷

¹²⁴ D. THÜRER, *Failing States*, in *Max Planck Encyclopedia of Public International Law*, Oxford, 2009. See also D. ACEMOGLU, J.A. ROBINSON, *Why Nations Fail. The Origins of Power, Prosperity, and Poverty*, London, 2012, where the reasons for the failure of international development aid are also examined (446 ff.).

¹²⁵ S.E. MERRY, K.E. DAVIS, B. KINGSBURY (eds.), *The Quiet Power of Indicators. Measuring Governance, Corruption, and Rule of Law*, Cambridge, 2015.

¹²⁶ F. FOER, *World Without Mind*, above, 6.

¹²⁷ I. CALVINO, *Se la parola non serve* (1977), in *Id.*, *Saggi* (1945-1985), Milan, 2001, II, 2332, here 2334 ff. (Author’s translation: “A democracy lives if the word is operative, that is, if criticism, denunciation, argumentation,

What are the remedies adopted against these risks? Once the strategic importance of big data, in this case relating to the profiling of billions of users, has been recognized, what scope for action remains for states?¹²⁸

The dilemma here concerns the relationship between public and private. In fact, in some countries, such as France, reference has been made to a phenomenon of “*privatization numérique*”, with “*la prise en charge par des entreprises de l'économie numérique de fonctions qui étaient traditionnellement réservées au secteur public entraînerat 'une recomposition du partage public-privé.*”¹²⁹

In the ultra-state sphere, it should be recalled that the global legal space has in the past already seen interventions by public authorities to correct or prevent possible distortions, inefficiencies, or dangers to the protection of fundamental rights arising from exclusively private regulatory regimes or frameworks.

In the field of sport, for example, the anti-doping programme is a case in which governments, after the scandals over the use of ‘doping’ substances that were rampant in the 1990s, built together with the IOC and the entire Olympic movement a new system of rules based on public-private cooperation mechanisms: the World Anti-Doping Code is approved by a Swiss foundation in which governments also participate, i.e. the World Anti-Doping Agency (WADA), and then adopted in all countries (which must also conform their laws to the Code by virtue of a specific UNESCO convention).¹³⁰ Another example is that of the rating agencies, where both the European Union and several countries have progressively imposed a series of rules on these private bodies, especially in view of the significant effects produced by their activities (i.e. the evaluation of the credit of states).¹³¹ Or think of the case of the Internet itself, with the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization governed by Californian law: this entity, as illustrated above, actually arose out of the US government’s need to cede control of the network; however, ICANN’s organization provides for a specific committee, the GAC, where representatives of all the states sit.¹³²

In the ultra-state sphere, therefore, the distinction between public and private performs several functions depending on the context.¹³³ The global legal space is a place where institutions, rules and procedures hybridize and intermingle: what is commonly framed as ‘public’ can take on ‘private’ traits and vice versa; the regulators, the states, are at the same time also the regulated;¹³⁴ the same phenomena can be observed through different lenses and referred to different traditions or discipli-

the demand for truth do not pass without leaving a mark. And it is only in this climate that the just word is not confused with the unjust or slanderous or empty word [...] the responsibility to say and to repeat what needs to be said grows with the hardening of the times”).

¹²⁸ A. ALEMANNI, *Big Data for Good*, above, 183.

¹²⁹ J. CHEVALLIER, *L'État en France. Entre déconstruction et réinvention*, Paris, 2023, 86; G. JEANNOT, S. COTTIN-MARX, *La Privatisation numérique. Déstabilisation et réinvention du service public*, Paris, 2022.

¹³⁰ L. CASINI, *Global Hybrid Public-Private Bodies: The World Anti-Doping Agency (WADA)*, in *International Organisations Law Review*, 6, 2009, 421 ff.

¹³¹ S. CASSESE, L. CASINI, *Public Regulation of Global indicators*, in K. DAVIS, A. FISHER, B. KINGSBURY AND S. ENGLE MERRY (eds.), *Governance by indicators: global power through quantification and rankings*, Oxford, 2012, 465 ff.

¹³² B. CAROTTI, *Il sistema di governo di Internet*, Milan, 2016.

¹³³ G. JURGENS, F. VAN OMMEREN, *The Public-Private Divide in English and Dutch Law: A Multifunctional and Context Dependant Divide*, in *Cambridge Law Journal*, 71, 2012, 172.

¹³⁴ J. WALDRON, *The Rule of International Law*, in *Harvard Journal of Law and Public Policy*, 30, 2006, 16.

nary spheres, traceable to international law, public law and private law.¹³⁵ Beyond the state, public law and private law find new combinations, mutually borrowing and exchanging institutions and solutions:¹³⁶ is the realm of intertwining and hybridization.¹³⁷

In such a framework, then, there is an urgent need to draw up international rules that can ensure high standards of protection of fundamental rights, foster the fight against disinformation and fake news, and guarantee the protection of personal data against all the large private companies that 'control' the web. When it comes to privacy, for example, or even defense against automated decisions, but also defense against so-called harmful contents, we need certain rules that are shared across the globe.

This seems to be the most important challenge awaiting the state and states in the 21st century, namely to somehow regain control over people's big data, at least in terms of global rules and guarantees for individuals and communities. Not surprisingly, it is the operators themselves who are asking for it, because they have understood the complexity and relevance of the problems they are now forced to deal with:¹³⁸ it is clear, for instance, that Meta or Google cannot be entrusted exclusively with the responsibility of moderating the contents of posts or messages during an electoral competition.

In this respect, the experience of the above mentioned Facebook Oversight Board is noteworthy, especially if one looks at the data presented in its first annual report (2021)¹³⁹ Out of approximately 1.1 million reports, after a selection process carried out by a special committee, the Board then decided on 20 cases, applying international human rights standards: in 14 of them the decision taken by Meta was changed, in six it was upheld. The Board also made around 90 recommendations to Meta, for instance asking the company to provide more information to users when removing a post, to translate its rules into the languages spoken by over 400 million people, to provide more details in response to government requests, to adopt crisis protocols to handle emergency situations, and to better inform users about whether a post was removed automatically or after checking by a human being.

In June 2023, the Board published its second annual report (2022).¹⁴⁰ Here it is noted that Meta implemented many of the recommendations made by the Board in 2022: for instance, it started telling people which specific policy their content violated when removing their content; it created a new section in the Community Standards on misinformation; it began systematically measuring the trans-

¹³⁵ See L. CASINI, *Down the Rabbit Hole: The Projection of the Public/Private Distinction Beyond the State*, in *International Journal of Constitutional Law*, 12, 2014, 402, and the bibliography cited therein.

¹³⁶ M. ROSENFELD, *Rethinking the Boundaries between Public Law and Private Law for the Twenty First Century: An Introduction*, in *International Journal of Constitutional Law*, 11, 2013, 125. Previously, M.J. HORWITZ, *The History of the Public/Private Distinction*, in *University of Pennsylvania Law Review*, 130, 1982, 1423.

¹³⁷ C. SCOTT ET AL, *The Conceptual and Constitutional Challenge of Transnational Private Regulation*, in *Journal of Law & Society*, 38, 2011, 1.

¹³⁸ See also the hearings of Jack Dorsey, Co-Founder and then Chief Executive Officer of Twitter, and Sheryl Sandberg, then Chief Operating Officer of Facebook, before the *US Senate Select Committee on Intelligence*, 5 September 2018 (<https://www.intelligence.senate.gov/hearings/open-hearing-foreign-influence-operations-use-social-media-platforms-company-witnesses>).

¹³⁹ <https://www.oversightboard.com/news/322324590080612-oversight-board-publishes-first-annual-report/>.

¹⁴⁰ <https://www.oversightboard.com/news/560960906211177-2022-annual-report-oversight-board-reviews-meta-s-changes-to-bring-fairness-and-transparency-to-its-platforms/>.

parency of its enforcement messaging to users; or introduced a new Crisis Policy Protocol. With 1.3 million reports (about a quarter more than in 2021), i.e. an average of one case every 24 seconds, there were 50 shortlisted cases (of which as many as 32 saw Meta’s decision reversed) and 12 were published. Furthermore, in October 2022, the Board announced seven strategic priorities “based on an extensive, in-depth analysis of the issues raised by user appeals to the Board”. They are elections and civic space; crisis and conflict situation; gender; hate speech against marginalised groups; government use of Meta’s platforms; treating users fairly; automated enforcement of policies and curation of content. Also in 2022, the Board issued its first advisory opinions.

The establishment and activity of the board so far offer some chiaroscuro points for reflection. On the one hand, the decision to activate such a body, whose main purpose is precisely to ensure greater transparency in the management and moderation of content on the Facebook platform, is to be welcomed. The data provided by the annual report are encouraging, and the decisions published so far are also a good starting point. On the other hand, Meta’s very decision to create its own control body once again confirms the mimicry between complex organizations and states. To some extent, the establishment of this committee is an attempt to organize itself better through the creation of a monitoring and dispute resolution power. One can find here the meaning of Zuckerberg’s well-known and above-mentioned statement that his company would be more like a government, or rather, we could say, a state with its own rules, its own “administration” and now also its own “judges”. If one looks at the history of the state and its dynamics, it would then seem that it is precisely the status of monopolists that favors the strengthening of these companies also in terms of differentiation of functions.¹⁴¹ And, still considering the historical perspective, it must be remembered that the exercise of ‘governmental’ functions by private entities or companies is not a new phenomenon: among the best known examples is the East India Company.¹⁴²

In this framework, it becomes essential to ensure that the public authorities have forms of intervention against G-tech companies. As mentioned above, there is first of all a sanctioning power, which has already been activated several times with reference to competition: take, for instance, the EUR 2.42 billion fine imposed by the EU Commission on Google in 2017 and whose legitimacy was confirmed by the EU General Court in November 2021.¹⁴³

Very relevant was the final approval by the European Parliament in June 2022 of the so-called ‘digital services package’ designed to limit the dominance and possible abuses of G-techs. These are the Digital Services Act (DSA) and the Digital Markets Act (DMA), to which must be added the Digital or Data Governance Act (DGA), focused on reuse and data security. The measures provided for by the DSA and the DMA include the obligation to ensure greater competition between services, but also the

¹⁴¹ The reference here is to N. ELIAS, *The Civilizing Process. Sociogenetic and Psychogenetic Investigations* (1969; 1994), transl., Oxford, 2017, 268 ff.

¹⁴² See W. DARLYMPLE, *The Anarchy. The Relentless Rise of the East India Company*, London, 2020. Similarly, one must remember the experiences of instruments aimed at entrusting the government of a territory or the subjugation of a population to individuals, as occurred with the Spanish “encomiendas” in America in the 16th century: see L. BYRD SIMPSON, *The Encomienda in New Spain: The Beginning of Spanish Mexico*, Berkeley and Los Angeles, 1982.

¹⁴³ <https://curia.europa.eu/juris/document/document.jsf?jsessionid=BBB2022ABF6D6108230F66A13703742A?text=&docid=249001&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=6495034>.

prohibition of dark patterns, i.e. those mechanisms aimed at manipulating users' attention and inducing them, for instance, to buy a certain product. To this end, the European measures intervene with various information obligations, also referring to the granting of consent by users.

Another important tool is tax leverage. In this regard, in 2021, the G20 signed an agreement on the so-called global tax, also to be applied to digital multinationals, to which 130 countries, representing 90% of global GDP, have adhered. In particular, the global tax, as defined by the OECD, rests on two pillars: it will have a minimum rate of 15% to be applied to multinationals with revenues over EUR 750 million and the taxable amount will be calculated on the profits made in the countries where these companies operate¹⁴⁴. The OECD has estimated the resources that will be reallocated to the markets where multinationals operate at around USD 100 billion a year. In addition, according to calculations by the European Network for Economic and Fiscal Policy Research almost \$40 billion will be paid by American G-techs: Amazon, Apple, Microsoft, Alphabet, Intel and Meta alone are expected to pay out close to \$28 billion.¹⁴⁵

From this framework emerges a central theme in state theory. We can recall here the interpretation of those scholars who have traced the formation of this type of political community to three fundamental principles of domination, understood as bases of social power: i.e. control of violence, control of information (or knowledge), and individual charisma (or charismatic politics).¹⁴⁶ The history and management of big data show that democratic states have progressively lost control of information or knowledge or they now have at least to share this domination with big tech companies. In this respect, one effect of the development of contemporary democracies on the state in the digital age is the profound change in the distribution of these three principles, identified as the "humble beginnings of sovereignty, bureaucracy and politics":¹⁴⁷ they are no longer entrusted to different public actors within the state, but to the state and multinational private actors. And this, as we have seen, has significant implications for the issue of truth and the formation of public opinion. And this is also the case when it is the states themselves that use platforms to disseminate information. In addition, it should be considered that "[m]any nations are - and are likely to remain indefinitely - reliant on network platforms that are both designed and hosted in other countries. Thus they are also likely to remain, at least in part, dependent on other countries' regulators for continued access, key inputs, and international updates."¹⁴⁸

Finally, a confirmation of how states today do not have full control over information and cannot fully exercise their "aleurgical" function comes from the events of the 2020 pandemic. In this case, the leading role acknowledged to states to counter the health emergency shows a certain line of continuity, in the exercise of public power and in the way it is perceived by populations, with the figure of the thaumaturge kings well described by Marc Bloch. In recounting one of the most resounding fake news in history, namely the rite of healing from scrofula by touching the hands of the Christian kings

¹⁴⁴ https://www.econpol.eu/press_releases/2021-07-05.

¹⁴⁵ <https://www.oecd.org/tax/beps/tax-challenges-arising-from-the-digitalisation-of-the-economy-global-anti-base-erosion-model-rules-pillar-two.htm>.

¹⁴⁶ D. GRAEBER, D. WENGROW, *The Dawn of Everything: A New History of Humanity* (2021), London, 2022, at 365, 390 and 413.

¹⁴⁷ D. GRAEBER, D. WENGROW, *The Dawn of Everything*, supra, 358.

¹⁴⁸ H.A. KISSINGER, E. SCHMIDT, D. HUTTENLOCHER, *The Age of AI: And Our Human Future*, London, 2021, 103.

of France and England in the Middle Ages, Bloch observes, with reference to Henry II Plantagenet, king of England (1133-1189), that “[s]on pouvoir guérisseur ne lui était pas personnel; il le tenait de sa fonction: c’est en tant que roi qu’il était thaumaturge.”¹⁴⁹ Thus, during the pandemic, the state became a “thaumaturge” in the widest possible sense: not only was it a “healer” by means of vaccination campaigns – on which, unfortunately, real battles of disinformation were unleashed – and even, as in the cases of China, Russia or Cuba, by directly promoting the production of its own vaccines; but the state also became a true insurer of last resort with respect to the economic-financial conditions of citizens and businesses. Unlike in the Middle Ages, the choices made by states to combat pandemics have been based on scientific elements and the support of technical bodies, even those set up *ad hoc*. However, public authorities have not always been able to implement information and communication strategies that are adequate to counter the disinformation produced more or less consciously through social networks: as Shoshana Zuboff pointed out, “these platforms are not bulletin boards but hyper-velocity global bloodstreams into which anyone may introduce a dangerous virus without a vaccine.”¹⁵⁰

As a matter of fact,

The dreams of the internet and digital technologies empowering citizens against dictatorship were not completely surreal. Digital technologies can be used for encryption, making it impossible for authorities to snoop in private communications. Services such as VPNs can be used to thwart censorship. Search engines such as Tor are currently impossible for governments to decrypt (so far as we know) and hence offer greater levels of privacy and security. Nevertheless, early hopes of digital democratization have been dashed because the tech world put its effort where the money and power lie – with government censorship. It is thus a specific path – a low road – chosen by the tech community that intensifies data collection and surveillance. Although advances in large-scale processing of data using tools from machine learning have been important in these efforts, the real secret sauce in surveillance by governments and companies in massive amounts of data.¹⁵¹

5.2. Institutions in the digital age: writing v. orality

In addition to the question of new Internet rules and the dialectic between public and private, there is another challenge awaiting the digital state, perhaps even more difficult, because it relates, in some ways, to the same logic with which public institutions are traditionally developed and consolidated.

The new technologies have also brought about profound changes in the way we communicate and enunciate. Writing (and in broader terms literacy), which has traditionally fostered the formation of

¹⁴⁹ M. BLOCH, *Les rois thaumaturges. Étude sur le caractère surnaturel attribué à la puissance royale particulièrement en France et en Angleterre*, Paris, 1983, 42. (Author’s translation: “his healing power was not personal to him; he possessed it by virtue of his function: he was a thaumaturge insofar as he was a king.”).

¹⁵⁰ S. ZUBOFF, *You Are Now Remotely Controlled. Surveillance capitalists control the science and the scientists, the secrets and the truth*, opinion in *The New York Times*, June 24, 2020 (<https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html>). See also D. KAYE, *Speech Police. The Global Struggle to Govern the Internet*, New York, 2019.

¹⁵¹ D. ACEMOGLU, S. JOHNSON, *Power and Progress*, above, 353.

institutions and political organizations with apparatuses,¹⁵² is now increasingly simplified and driven by mimetic logics of orality: one only has to see the increasing diffusion of WhatsApp voice messages or stories posted on Instagram or videos on Tik-Tok.

Thus, there is a progressive reduction or even elimination of the different levels of reading of a text. Likewise, in-depth analysis is lost and argumentation as the main form of motivation for decisions is abandoned. As has been observed, after all, (early) writing is “inextricably bound to state making.”¹⁵³

It is no coincidence that Yuval Noah Harari, in his best-seller “Sapiens”, devoted pages to the “wonders of bureaucracy” related to the development of written language in Mesopotamia.¹⁵⁴

What consequences might these changes have for the democratic state?

History shows that the “myth of the state” has always been accompanied by a “transformation of human speech”, where “[t]he magic word takes precedence of the semantic word.”¹⁵⁵ The technological revolution – which profoundly affects writing, memory and modes of communication and storage – and ‘surveillance capitalism’ seem to have produced a new language,¹⁵⁶ with totalitarian ambitions.¹⁵⁷ These are possible consequences of the shift “from ‘facts’ to ‘data’”¹⁵⁸, also favored by Facebook and Google when they aim to anticipate our decisions: it is, as has been pointed out, the new “Data religion” or “dataism”, according to which “the universe consists of data flows, and the value of any phenomenon or entity is determined by its contribution to data processing.”¹⁵⁹

The digital revolution, therefore, also arises as a “graphic revolution”, which

*excède donc l'apparition d'une nouvelle forme d'écriture dans la mesure où le changement technique a des effets puissants sur la perception du monde et des autres, et sur la constitution de ce qui fait valeur. Le numérique n'est pas seulement une nouvelle écriture, qui rendrait la diffusion et la circulation d'un message plus rapide et de manière dématérialisée, donc déterritorialisée; elle a des conséquences plus profondes parce qu'elle est également une révolution symbolique. [...] Un changement d'époque, c'est-à-dire une transformation des modes de constitution du sens qui affecte à la fois la perception des objets et des valeurs, et modifie leurs représentations. Le numérique agit comme un réorganisateur symbolique affectant tous les secteurs de la vie aussi bien subjective, qu'intersubjective et collective. Son impact sur le droit est particulièrement révélateur des nouveaux enjeux de cette révolution car celui-ci est par nature le lieu de l'élaboration collective des normes qui a vocation à encadrer toute activité sociale.*¹⁶⁰

¹⁵² The point is well made by J. DIAMOND, *Guns, Germs and Steel. A brief history of everybody for the last 13,000 years* (1998), London, 2017, 234 ff. See also the studies done by W.V. HARRIS, *Ancient Literacy*, Cambridge, 1991, and, earlier, by J. GOODY, *The Logic of Writing and the Organisation of Society*, 1986, 87 ff. (where the relations between state, bureau and file are examined).

¹⁵³ J.C. SCOTT, *Against the Grain: A Deep History of the Earliest States*, New Haven, 2017, 146. By the same author, ID., *The Art of Not Being Governed: An Anarchist History of Upland Southeast Asia*, New Haven, 2009, in particular 220 ff, where the relationships between orality, writing, texts and stateless populations are analysed.

¹⁵⁴ Y.N. HARARI, *Sapiens. A Brief History of Humankind*, New York, 2011, 126 ff.

¹⁵⁵ E. CASSIRER, *The Myth of the State*, supra, 278.

¹⁵⁶ The reference is to S. ZUBOFF, *The Age of Surveillance Capitalism*, above.

¹⁵⁷ É. SADIN, *Surveillance globale. Enquête sur les nouvelles formes de contrôle*, Climats, 2009.

¹⁵⁸ W. DAVIES, *Nervous States*, supra, 175 ff.

¹⁵⁹ Y.H. HARARI, *Homo Deus. A Brief History of Tomorrow* (2015), 2017, chapter 11. See also B. KAISER, *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*, 2019.

¹⁶⁰ A. GARAPON, J. LASSÈGUE, *Justice digitale: Révolution graphique et rupture anthropologique*, above, 29 ff. (Author's translation: “The impact of digital technology goes beyond the appearance of a new form of writing, in-

The precedents of such revolutions are not always encouraging, because the so-called “co-opting of language” is a typical trait of authoritarian regimes: think of the neo-language used in George Orwell’s dystopia 1984 or the so-called Ur-fascism analyzed by Umberto Eco.¹⁶¹

What is the future of the state then? How is this type of political organization conditioned by the creation and development of a frenetic, syncopated, non-argumentative language?

Those outlined here are just some of the working hypotheses that can be followed to pursue the study of these topics, provided, however, that one does not remain ‘in love’ with the word and concept of the state without observing the transformations of reality.¹⁶² Brecht’s Mr. Keuner must always be remembered when studying these phenomena:

“What do you do”, Mr. K. Was asked, “if you love someone?”

“I make a sketch of the person”, said Mr. K, “and make sure that one resembles the other.”

“Which? The sketch?”

“No”, said Mr. K., “the person.”¹⁶³

sofar as technical change has powerful effects on our perception of the world and of others, and on the constitution of what constitutes value. Digital technology is not just a new form of writing that makes it possible to disseminate and circulate a message more quickly and in a dematerialised, and therefore deterritorialised, way; it has more far-reaching consequences because it is also a symbolic revolution. [...] An epochal change, in other words a transformation of the ways in which meaning is constituted, affecting both the perception of objects and values, and modifying their representations. Digital technology acts as a symmetrical reorganiser, affecting every sector of subjective, intersubjective and collective life. Its impact on the law is particularly revealing of the new challenges posed by this revolution, as the law is by its very nature the place where standards are collectively drawn up to provide a framework for all social activity.”) See also C. HERRENSCHMIDT, *Les trois écritures. Langue, nombre, code*, Paris, 2007.

¹⁶¹ M. KAKUTANI, *The Death of Truth: Notes on Falsehood in the Age of Trump*, New York, 2018; U. Eco, *Il fascismo eterno* (1997), Milan, 2017.

¹⁶² Not least because the doctrine of the state is the science of reality: H. HELLER, *Staatslehre*, Leiden, 1934.

¹⁶³ B. BRECHT (1898-1956), *Stories of Mr. Keuner*, transl., San Francisco, 2003, 27 (The original German text from B. BRECHT, *Geschichten vom Herrn Keuner*, Berlin, 2011, 45, is the following: “Was tun Sie”, wurde Herr K. gefragt, “wenn Sie einen Menschen lieben?” “Ich mache einen Entwurf von ihm”, sagte Herr K., “und Sorge, daß er ihm ähnlich wird.” “Wer? Der Entwurf?” “Nein”, sagte Herr K., “der Mensch.”)