Received: 11 March 2021 | Revised: 23 April 2021 | Accepted: 23 April 2021

DOI: 10.1111/eulj.12388

ORIGINAL ARTICLE

WILEY

Making the digital economy "fit for Europe"

Andrea Renda*

Abstract

Over the past three decades, cyberspace has gradually become an engine of unsustainable outcomes from an economic, social and environmental perspective. The European Commission has launched several new initiatives, in the attempt to restore public control over cyberspace, remedy the distributional imbalances generated by the rise of large-scale digital platforms, and promote Europe's digital sovereignty. The paper argues that only by embedding rules and values in "code" and preserving openness towards the rest of the world will the EU manage to achieve its desired goals. Current initiatives such as the data strategy, the AI regulation, the Digital Services Act and the European Cloud Federation appear still too sparse and uncoordinated to really deliver on Europe's ambition to lead the world in the sustainable use of technology.

1 | INTRODUCTION: THE UNSUSTAINABLE LIGHTNESS OF CYBERSPACE

Three decades after its first steps into our lives, the World Wide Web has become an impregnable fortress, barely scratched by lawmakers' attempts to establish the rule of law—a fortress further ring-fenced by the COVID-19 pandemic, which transformed it from a parallel universe to an unavoidable, essential access point to the reality around us. The dizzying increase in *online* Internet traffic observed over the past months drew a definitive blow to the stances of those (indeed, fewer and fewer) who resisted the idea that the Internet has turned, from playground for selected techies, into a critical infrastructure including the energy network, the banking system and the agri-food chain; and that access to the "network of networks" should be configured as a constitutionally protected right, to be pursued with highest priority so as to avoid outcomes where entire portions of territory and population end up being discriminated and excluded, contradicting the goal of "leave no one behind", so dearly and meaningfully embraced by advocates of sustainable development.[1]

* Professor of Digital Policy, EUI School of Transnational Governance, Senior Research Fellow and Head of Global Governance, Regulation, Innovation and the Digital Economy (GRID), Centre for European Policy Studies; andrea.renda@eui.eu

[1]See United Nations Commission for Social Development Fifty-Ninth Session, 2nd Meeting, at https://www.un.org/press/en/2021/soc4890.doc.htm. See also, J. Roese, 'COVID-19 exposed the digital divide. Here's how we can close it', *World Economic Forum*, 27 January 2021.

Today, we increasingly call on the digital infrastructure, and even more on the giants that dominate it, to protect our democracies battered by populism and disinformation, as well as to support and revive our economy, revitalise our social relations weakened by the lockdown age, and unleash the transformation of our economic system towards new shores of resilience and sustainability. The European Union is now officially pursuing a "twin" transition (green and digital), in its quest for resilient and sustainable recovery after the pandemic.[2] Yet, relying on the digital ecosystem as a thaumaturge of the distortions and difficulties of the real world may also be seen as an acrobatic, if not paradoxical, attempt. To some extent, the almost blind reliance on technological solutions, such as contact-tracing apps at the beginning of the COVID-19 pandemic, shows how puzzling and awkward the relationship between governments and digital technologies still is.[3] As a matter of fact, beyond its thrills and wonders, cyberspace today is also a paradigmatic example of unsustainability. It suffices to look back a few years to realise that the magnificent promise of the Internet has remained largely written in a book of dreams, nurtured by the rhetoric of laissez-faire that inspired the founders of the Web from the very outset. The phenomenal thrust of the early, anarchic days of the Internet has inevitably put the legislator in the passenger seat, deprived of control, spectator of the triumphant rhetoric of permissionless innovation (a stance that is currently resurfacing, almost unchanged, when it comes to smart contracts and distributed ledger technologies).[4]

The *Cahier de doléances* is dense, and encompasses economic, social and to some extent also environmental considerations. First, economic unsustainability emerged as a result of the extraordinary concentration of economic power in the hands of a fistful of entities. These entities feature an alternative, hybrid *governance*, combining elements of the traditional "firm", as theorised by academics such as Ronald Coase and Oliver Williamson, and some of the elements of market exchanges.[5] So-called "platforms" bear little resemblance to the structure and features of firms as contemplated by the civil and commercial laws of most countries around the world. Thanks to the centripetal dynamics caused by network externalities in the Internet's end-to-end architecture, these entities were capable of capturing a large part of the value generated by the digital ecosystem[6]; yet, they are at the same time able to outsource and externalise almost all business functions, including monitoring employee performance, as well as verifying compliance with the legislation by the products and services that pass through it, generating attractive advertising opportunities and swaths of data that, once aggregated, generate substantial value. Already a few years ago, a study compared the "Big 3" car manufacturers (GM, Ford and Chrysler) in 1990 with Silicon Valley's "Big 3" (Google, Apple and Facebook) in 2014, and found that the tech giants had nine times fewer employees and were worth 30 times more on the stock market: with the pandemic, this anomaly has become even more macroscopic.[7]

As is well known, large online intermediaries have remained shielded from legally imposed liability with regard to most of the impact that their activity exerts on society, the economy and the environment, as well as on the democratic process. To be sure, this initially responded to the need to preserve the neutrality of the Internet, preserving it as a locus of free exchange of information between users, in line with the end-to-end architecture of the Internet.[8]

---

[2]See, for example, the speech by President Ursula Von der Leyen on the State of the Union of 16 September 2020, in which it is reiterated that the Commission is aiming for a "twin green and digital transition", SPEECH/20/1655.

[3]For an analysis, see A. Renda, 'Covid-19 and Privacy: a European Dilemma', TRIGGER Working Paper (2020), at https://trigger-project.eu/2020/04/08/covid-19-and-privacy-european-dilemma/; see also, World Health Organization, 'Contact tracing in the context of COVID-19: interim guidance', 1 February 2021, at https://apps.who.int/iris/handle/10665/339128.

[4]See, among others, H. Chesbrough and M. Van Alstyne, 'Permissionless Innovation', (2015) 58 *Communications of the ACM*, 24–26; V. Cerf, 'Keeping the Internet Open', (2016) 59 *Communications of the ACM*, 7; and the contribution of Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press, 2006).

[5]See R. Coase, 'The Nature of the Firm', (1937) 4 *Economica*, 386–405. O.E. Williamson, *Markets and Hierarchies: Analysis and Anti-Trust Implications* (Free Press, 1975). See also, K. Reimers, X. Guo and M. Li, 'Beyond Markets, Hierarchies, and Hybrids: An Institutional Perspective on IT-enabled Two-sided Markets', (2019) 29 *Electron Markets*, 287–305.

[6]See, among others, D. Autor, D. Dorn, L.F. Katz, C. Patterson and J. Van Reenen, 'The Fall of the Labor Share and the Rise of Superstar Firms', (2020) 135 *The Quarterly Journal of Economics*, 645–709.

[7]R. Dobbs, A. Madgavkar, J. Manyika, et al., 'Poorer Than Their Parents? Flat or Falling Incomes in Advanced Economies' (McKinsey Global Institute, 2016).

[8]M.A. Lemley and L. Lessig, 'The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era', (2001) 48 *UCLA Law Review*, 925; A. Renda, 'Competition, Neutrality and Diversity in the Cloud', (2012) 85 *Communications & Strategies*, 23–44; A. Renda, 'Net Neutrality and Mandatory Network-Sharing: How to Disconnect the Continent', *CEPS Policy Briefs*, 18 December 2013; and A. Renda, 'Antitrust, Regulation and the "Neutrality Trap"', *CEPS Special Report* no. 104, April 2015.

Today, however, the situation has changed considerably: the Internet (or at least its visible part) is in the hands of a few subjects who control information flows in a very pervasive way, governing the attention of end users (hence the name of "attention merchants" used by Tim Wu, now member of the National Economic Council in the US Biden-Harris administration) and extracting a substantial portion of the value generated. The result is obvious: the (two) trillion dollar companies, whose valuation further multiplied even before the pandemic, were already worth more than the entire European stock market.[9] Already at the beginning of 2020, big techs were worth $2 trillion more than the media sector.[10] This concentration of value in a few hands is unsustainable for all economic actors who see a growing dependence on the giants of the Web, with consequent transfer of value to the latter's advantage (think of the 30% toll imposed by Apple on those businesses that use its store to reach consumers).[11]

A corollary of this situation is the deterioration of the innovative capacity of smaller companies, gradually deprived of the necessary resources to invest in research and development, as well as frustrated in their ambitions by an increasingly penalising market context. Even the International Monetary Fund has started to report a worrying trend, with market concentration rising in many sectors along with mark-ups and profits, which are not being sufficiently converted into investment.[12] The problem of "value capture", denounced among others by Mariana Mazzucato, has become a hot topic on the most exclusive and influential political tables, and even turned into a geopolitical problem (given that the platforms are essentially American or Chinese), with the United States and China themselves grappling with a problem of internal distribution of economic value, to the point that they, too, are starting to implement more stringent forms of regulation.[13]

But the unbearable lightness of digital platforms does not end with economic considerations. Beyond the perimeter of profits and losses, the precariousness and devaluation of human work in an increasingly algorithmic context appears as a dystopian, yet very realistic scenario. A recent ILO flagship publication of the International Labour Organisation highlighted the progressive deterioration of the conditions of workers in many digital platforms, as labour contracts are replaced by a network of short-term, extremely precarious contracts.[14] Moreover, an analysis of working conditions governed by algorithms projects even more apocalyptic scenarios, with entire squads of workers employed to train machines that one day, thanks to such training, will finally be able to do without them.[15]

The unsustainability of cyberspace also has environmental implications, in particular as regards the energy consumption of data centres and deep learning systems, which require huge amounts of energy to be properly trained.[16] Even more evident is the case of peer-to-peer network technologies which, in order to guarantee information redundancy, require continuous synchronisation between nodes and complex cryptographic procedures for validating transactions, thus requiring disproportionate amounts of energy (think of the blockchain, which to date is estimated to consume more energy than countries like Argentina).[17] Work by the International Telecommunications Union

[9]See T. Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Vintage Books, 2017). In fact, FAANGS stocks in 2018 were instrumental in bringing back equity index values that otherwise would have been significantly negative. See, also, J. Pound, 'US Tech Stocks Are Now Worth More Than the Entire European Stock Market', *CNBC*, 28 August 2020, available at https://www.cnbc.com/2020/08/28/us-tech-stocks-are-now-worth-more-than-the-entire-european-stock-market.html; and J. Jolly, 'Is Big Tech Now Just Too Big to Stomach?', *The Guardian*, 6 February 2021, available at https://www.theguardian.com/business/2021/feb/06/is-big-tech-now-just-too-big-to-stomach.

[10]See G. Bridge, 'Big Tech Is Now Worth $ 2 Trillion More Than Media Sector', *Variety*, 3 January 2020, available at https://variety.com/2020/biz/news/big-tech-is-now-worth-2-trillion-more-than-media-sector-1203456031/.

[11]See the start of the European investigation in the *Spotify* case *v. Apple*, and the commentary by D. Geradin and D. Katsifis, 'The Antitrust Case Against the Apple App Store', available at https://ssrn.com/abstract=3583029. Similar is the controversy between Epic Games (video game producer, including the famous *Fortnite*) and Apple, which, after various skirmishes, resulted in an appeal to the European Commission by Epic Games on 17 February 2021.

[12]See International Monetary Fund, *World Economic Outlook Report*, April 2019.

[13]See M. Mazzucato, *The Value of Everything: Making and Taking in the Global Economy* (Public Affairs, 2018). On the same theme, with a focus on P AESI developing, an extensive report was published in 2019 by UNCTAD, 'Value Creation and Capture: Implications for Developing Countries', Digital Economy Report, 2019. See also, D.J. Teece and G. Linden, 'Business Models, Value Capture, and the Digital Enterprise', (2017) 6 *Journal of Organization Design*, 8.

[14]See ILO, 'The Role of Digital Labour Platforms in Transforming the World of Work', *World Economic and Social Outlook Report* 2021.

[15]See also H. Hauben, K. Lenaerts and S. Kraatz, 'Platform Economy and Precarious Work: Mitigating Risks', Briefing for the committee on Employment and Social Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.

[16]See N. Jones, 'How to Stop Data Centres from Gobbling Up the World's Electricity', (2018) 561 *Nature*, 163–166; E. Strubell, A. Ganesh and A. McCallum, 'Energy and Policy Considerations for Deep Learning in NLP', (2019) *ArXiv*, abs/1906.02243.

[17]See C. Criddle, 'Bitcoin Consumes "More Electricity than Argentina"', *BBC News*, 10 February 2021, available at https://www.bbc.com/news/technology-56012952.

recently highlighted that compliance with the Paris Agreement will require the industry to reduce greenhouse gas emissions by 45% by 2030, mostly through a shift to renewable and low-carbon energy.[18] A recent review of available estimates concluded that "under business as usual, the most optimistic projection sees ICT's emissions staying stable at the current level", and that ICT will not reduce its emissions without a major concerted effort involving broad political and industrial action.[19]

Several other aspects of the digital economy show traces of growing unsustainability. On the one hand, cybersecurity is an ever-shifting frontier, especially when one thinks of the rise of the Internet of Things, which exposes networks to a growing threat of cyberattacks by making the attack surface denser and more porous every day.[20] On the other hand, the promises of work automation and the transformation of value chains risk excluding entire countries from the global economy, even more so today that *re-shoring* becomes a possible and necessary perspective to obviate the country-risk induced by the pandemic.[21] In this context, the digital divide continues to penalise entire portions of territory, even within the EU, potentially setting up a loss of opportunity for all citizens that reside in areas that are least served by digital services and connectivity.

Finally, the lack of effective control of the governance of the network by public institutions involves increasingly evident problems also for the stability of the democratic process. Those who were shocked by the Cambridge Analytica scandal, which exposed for the first time the disturbing world of behavioural experiments that social networks conduct every day on unaware masses of users, must today surrender in the face of the spread of algorithmic practices that are deployed with very limited accountability, not only in the private sector but also in government. Recent cases such as those involving algorithms like Syri and Gladsaxe in European countries, and COMPAS in the United States show that the relationship between governments and their citizens has now reached a "red alert" level when it comes to AI deployment, and that the potential benefits of digital government need to be carefully scrutinised to ascertain that the modus operandi of AI systems does not violate basic fundamental rights, as well as the provisions of administrative law and the right to good administration.[22]

As a result, there are no grounds for claiming the primacy of public governance over private governance (of platforms): rather, both sides risk plunging society into an unsustainable, technology-driven dystopia, if they do not equip themselves with instruments of transparency, democratic control and accountability when using AI systems and applications. And although it is certainly true that digital technologies, by their intrinsic characteristics, are both a cause and a solution to this problem, the fact remains that reliance on free market forces has led so far to unsustainable results, rather than driving meaningful progress.[23] In this continuous evolution, already exacerbated by the pandemic, a symbolic point of no return is represented by the attack on the US Capitol Hill in January 2021, followed by the unilateral decision of Twitter and Facebook to permanently ban from their communities the (then) President of the United States. A culminating moment in which many of the problems raised in the previous pages are easily spotted: the manipulation of social networks for political use, the absence of full responsibility on the part of intermediaries, the triumph of private governance, without any legal instrument in place to effectively constrain the conduct of digital platforms. A worrying scenario that has disturbed the sleep of European legislators for quite

[18]See ITU, GeSI GSMA and the Science Based Targets Initiative, 'Guidance for ICT Companies Setting Science-based Targets' (2020), available at https://www.itu.int/en/mediacentre/Documents/Documents/GSMA_IP_SBT-report_WEB-SINGLE.pdf

[19]See C. Freitag, M. Berners-Lee, K. Widdicks, B. Knowles, G. Blair and A. Friday, 'The Climate Impact of ICT: A Review of Estimates, Trends and Regulations', (2021), available at https://arxiv.org/abs/2102.02622.

[20]See, among others, S. Rizvi, R.J. Orr, A. Cox, P. Ashokkumar and M. Rizvi, 'Identifying the Attack Surface for IoT Network',(2020) 9 *Internet of Things*, 100, 162.

[21]See, for a pre-pandemic view, D. Rodrik, D. 'New Technologies, Global Value Chains, and the Developing Economies', Pathways for Prosperity Commission Background Paper Series no. 1. Oxford (2018). More recently, the issue of the impact of the post-pandemic digital transformation on developing countries was tackled by A. Korinek and J.E. Stiglitz, 'Artificial Intelligence, Globalization, and Strategies for Economic Development', NBER Working Paper No. 28453 (2021).

[22]M. Choroszewicz and B. Mäihäniemi, 'Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries', (2020) 1 *Global Perspectives*, 12,910. For a comparative overview, see also G. Misuraca and C. van Noordt, *Overview of the Use and Impact of AI in Public Services in the EU* (Publications Office of the European Union, 2020).

[23]For an analysis of the solutions and problems associated with AI technology in the achievement of the SDGs, see R. Vinuesa, H. Azizpour, I. Leite, I. et al., 'The Role of Artificial Intelligence in Achieving the Sustainable Development Goals', (2020) 11 *Nature Communications*, 233.

some time and is now beginning to worry policy-makers in the United States, Japan and China, with a rising, sneaky feeling: that in the quest for permissionless innovation, we ended up legitimising the spread of equally permissionless surveillance.[24]

2 | FROM LEGAL CODES TO SOFTWARE CODES: MAKING THE DIGITAL ECONOMY "FIT FOR EUROPE"

The European emphasis on the digital transformation as a salvific tool for sustainable post-pandemic recovery crucially requires action to bend cyberspace to the needs of protecting the fundamental principles and values of European law. This is even more important since, beyond the challenges already highlighted, Europe also faces a geo-economic problem, due to the fact that none of the platforms that dominate the Web is European, and yet platforms thrive thanks to the data and behaviour of European individual and business users.[25] The value capture problem is therefore tinged with double meaning: on the one hand, there is a need for a redistribution of value; on the other hand, EU leaders attempt to achieve also a "repatriation" of data, or at least the chance that future data produced by citizens and industry do not depart from Europe to land on American and Chinese shores.

The need for a distinctive European approach to digital policy, however, appears as evident in theory as it is incredibly complex to realise in practice. The poster child of the past years of "Brussels effect", the EU General Data Protection Regulation (GDPR), has certainly had the merit of relaunching the role of public authorities in "interfering" with the constant evolution of cyberspace[26]; however, it also showed the ability of big techs to circumvent the obstacle.[27] To date, the GDPR compliance rate seems to be rather low, and even where data processors strive to comply with the provisions of the GDPR, the goal of empowering end users with greater control over their personal data has remained unattained.[28] Thus, as lawmakers around the world, from Brazil to Japan and even California, rush to copy the GDPR model, it is gradually becoming self-evident that a traditional approach to regulation, based essentially on *ex post* control by courts and regulatory agencies, can only scratch the surface of a subject matter that travels at the speed of light, and hides patterns of compliance (or lack thereof) under a thick veil of code. The so-called "pacing problem", which scholars highlighted with respect to all disruptive technologies, here calls for new forms of adaptive regulation, which may require the introduction of new tools, and more agile forms of governance.[29]

Against this backdrop, the European Union has gradually changed its vision of the digital single market, acting on various fronts and with different tools to "tame" cyberspace to the need for the protection of fundamental rights, the requirements of the Green Deal, as well as to the European ambition of greater technological sovereignty and open strategic autonomy.[30] One telling example is the proposed "Regulation on a European Approach to Artificial Intelligence", adopted by the European Commission on 21 April 2021, which represents the first-ever attempt to

[24]See, among others, S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future and the New Frontier of Power* (Public Affairs, 2019), 691. See, also, C. You, 'Law and Policy of Platform Economy in China', (2020) 39 *Computer Law & Security Review* (China later disclosed guidelines for dealing with platforms in national antitrust legislation in November 2020). In 2020, Japan adopted a law on improving transparency and fairness in the commercial practices of some specific digital platforms, which closely recalls the European P2B regulation.

[25]See the recent European Commission Communication, '2030 Digital Compass: the European Way for the Digital Decade', COM(2021)118 final, in which the Commission observes that 90% of the EU's data are managed by US companies, and less than 4% of the top online platforms are European.

[26]See A. Bradford, *The Brussels Effect* (Oxford University Press, 2019).

[27]See the 2019 Capgemini Research Institute Report entitled 'Championing Data Protection and Privacy—A Source of Competitive Advantage in the Digital Century', which highlights that companies have adhered to the regulation more slowly than expected, citing how the complexity of regulatory requirements, implementation costs, and legacy infrastructure challenges have hindered progress. According to Capgemini, just 28% of the companies interviewed had managed to fully meet the requirements of the legislation one year after its entry into force.

[28]See I. van Ooijen and H.U. Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioral Perspective', (2019) 42 *Journal of Consumer Policy*, 91–107.

[29]See G. Marchant, B. Allenby and J. Herkert (eds.), '*The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Springer, 2011).

[30]For a more complete analysis of the impact of these initiatives on the technology stack, see A. Renda, 'Single Market 2.0: The European Union as a Platform', in S. Garben and I. Govaere (eds.), *The Internal Market 2.0* (Bloomsbury, 2020).

develop a comprehensive framework for the regulation of Artificial Intelligence.[31] In this proposal, the European Commission took an extremely bold stance on the prohibition of certain uses of AI, and proposed an ambitious approach based on the ex ante assessment of the riskiness of AI products, coupled with rather strong post-market surveillance and ex post enforcement provision, in a framework that fully captures the legacy of the GDPR (including in the governance mechanisms proposed, e.g. an AI Board).

Beyond these developments, a number of new trajectories are becoming apparent. The following appear to be particularly relevant.

First, EU institutions, pushed by some Member States, are working on a gradual and progressive redefinition of the scope of application of competition rules. The need to revisit traditional antitrust law instruments had already emerged in the past, particularly during the years of the US and EU Microsoft cases, dating back to the 1990s and early 2000s.[32] In the following years, while the main principles of antitrust law have remained valid, the tools and proxies used by competition authorities have gradually proven less and less effective and fit for purpose, because they echo the structure and dynamics of the "analogue" market economy.[33] Thus, in the domains of abuse of dominance and merger control, and even with regard to cartels with the emergence of algorithmic forms of collusion, the use of competition law to promote a dynamic economy as well as social welfare has gradually lost its teeth, causing a change of direction—at least in embryonic form—which has started to surface in some new proposals for ambitious EU legislation.

This is leading to a spectacular U-turn inside the European Commission. After years in which DG COMP pursued the "downward" harmonisation of national competition law, through the elimination of regulations on unilateral conduct that were widespread at national level but absent in EU law, over the past few years the need to make antitrust law more flexible to capture situations of abuse of economic dependence, superior bargaining power or "relative dominant positions" has emerged more strongly.[34] This has resulted in both an expansion of ex post control beyond the traditional antitrust perimeter (e.g., overcoming the subtleties of market definition and even proof of abuse, as in the recently proposed Digital Markets Act); and a transition from ex post control towards ex ante forms of regulation (think of the Platform-to-Business or P2B regulation, and more recently the proposed Digital Services Act).[35]

In this new context, so-called gatekeepers are given a "special responsibility" similar to that previously attributed to super-dominant companies, such as the owners of essential infrastructure or assets, in line with the essential facilities doctrine,[36] with a double result: on the one hand, the liability regime of digital intermediaries is tightened with respect to the fairness and transparency of the conditions they apply to businesses using their platforms; on the other hand, more than favouring the contestability of the market, the sought interventions end up focusing more convincingly on intra-platform competition, and thus on crystallising the centrality of existing large platforms, rather than seeking to create the preconditions for new platforms to emerge over time.

A second trend that is emerging in EU policy is the gradual overcoming of the principle of net neutrality, which has so far translated into an absence of responsibility of intermediaries for the conduct of their users. As cyberspace becomes a critical infrastructure for the economy and society, the principle of neutrality (already largely

[31]Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, Brussels, 21.4.2021.

[32]See R. Pardolesi and A. Renda, 'The European Commission's Case Against Microsoft: Kill Bill?', (2004) 27 *World Competition*, 513.

[33]See the study for the European Commission by J. Crémer, H. Schweitzer and Y.-A. de Montjoye, *Competition Policy for the Digital Era* (European Union, 2019).

[34]See D. Kalff and A. Renda, *Hidden Treasures: Mapping Europe's Sources of Competitiveness Advantage in Doing Business* (CEPS, 2020). See also, with reference to the previous orientation of the Commission—which aimed to extend to Art. 102 the convergence already foreseen for Art. 1010 by regulation 1/2003—A. Renda A. et al. (2012), 'The Impact of National Rules on Unilateral Conduct that Diverge from Article 102 TFEU', Study for the European Commission, DG COMP (2012); and A. Renda A. et al., 'Legal Framework Covering Business-to-Business Unfair Trading Practices in the Retail Supply Chain', Study for the European Commission, DG MARKT (2014).

[35]Reference is made to Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 which promotes fairness and transparency for commercial users of online intermediation services, OJ L 186 of 11.7.2019, 57–79. And to the Proposal for a Regulation of the European Parliament and of the Council on fair and contestable markets in the digital sector (law on digital markets), COM/2020/842 final.

[36]See, among others, A. Renda, 'Competition-Regulation Interface in Telecommunications. What's Left of the Essential Facilities Doctrine?', (2010) 34 *Telecommunications Policy*, 23–35; and E.A. Valdivia, 'The Scope of the "Special Responsibility" upon Vertically Integrated Dominant Firms after the Google Shopping Case: Is There a Duty to Treat Rivals Equally and Refrain from Favouring Own Related Business', (2018) 41 *World Competition*, 43–68.

circumvented in cyberspace) is no longer easy to justify, unless one accepts the creation of an immense grey area in the enforcement of public policy. The result, once more, is a move in the direction of greater public control over digital platforms. Yet, while in the UK the debate initiated by the White Paper on online harms is leading towards more pervasive statutory responsibility on the side of big platforms, the proposed Digital Services Act (DSA) maintains, though with many exceptions, the exemption from responsibility already contained in the e-commerce directive. In this respect, the DSA is still in continuity with a generation of public policy in which the intrusion of intermediaries in the content exchanged by users was considered heretical and eccentric with respect to the material constitution of cyberspace.[37] However, very large platforms are now being asked to put in place stringent measures to ensure the correct and legitimate development of social relations and economic life in their ecosystems. This includes, at least in the Commission proposal, the possibility of inspections on the algorithms used to profile users and order the results of individual searches—a possibility, however, difficult to translate into practice given the limited availability of specific skills in the control authorities.[38]

In this respect, the DSA does not seem likely to overcome the decade-long paradox of EU law, in which the same entities that are almost demonised by policy-makers (the so-called "GAFTAM") are also asked to contribute to the enforcement of EU rules through algorithmic take-down in contexts that are extremely delicate from the standpoint of fundamental rights, such as those on hate speech or on the protection of copyright.[39] The needed step forward, as will be recalled in more detail below, cannot but contemplate rather invasive forms of real-time inspection of the functioning and behaviour of the algorithms deployed by intermediaries. At present, except for what will be said below, EU institutions seem very far from developing this technology-enabled vision of law, let alone proceeding towards its concrete implementation.

A third trajectory that deserves notice is the need to propose technological solutions and technical protocols that embed compliance with regulatory provisions as design features. The failure of the traditional mechanisms of application of the law, from the regulatory authorities to the judges, requires that legislators make an effort towards adapting their tools to the digital economy: in other words, an effort at speaking the same language as the underlying regulated subject matter. Therefore, forms of algorithmic regulation are likely to become almost inevitable, with all the caveats of the case: if artificial intelligence errs in the private sector, it can certainly also create damages in public policy.[40]

From this point of view, a dazzling but still embryonic example is the EU attempt to counter the excessive power of the cloud giants, not by favouring the emergence of a European giant cloud provider, but through a European cloud federation, a jumble of technical protocols to be compulsorily applied to anyone who wants to provide cloud services in the EU; such a federated cloud would impose compliance with European regulation (first and foremost, the GDPR) "by design". In this context, legal codes become computer codes; contractual and regulatory specifications are translated into interfaces and protocols.[41] The principle (more than its implementation) is simple: it is enough to recall what Lawrence Lessig admirably anticipated already in the mid-nineties—that in cyberspace "code, not law, defines what's possible" (and what is perceived as lawful).[42] And that the law can really influence the conduct of cyberspace players only if it permeates in-depth the "stuff bits are made of", i.e. code. The European attempt to create a federated cloud, based on the Franco-German GAIA-X initiative, therefore promises to revolutionise the

[37]See the UK's 'Online Harms White Paper', available at https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper. And the Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (law on digital services), amending Directive 2000/31/EC, COM(2020) 825 final, 15 December 2020.

[38]See Art. 21(3) of the Proposal for a Regulation of The European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, SEC(2020) 432 final; and Art 19(1) of the Proposal for a Regulation of The European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), SEC(2020) 437 final.

[39]See, among others, M. Lambrecht, 'Free Speech by Design—Algorithmic Protection of Exceptions and Limitations in the Copyright DSM Directive', (2020) 11 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 68, para. 1.

[40]For numerous examples, see A. Renda, M. Laurer and N. Iacob, 'Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe', (2021) *CEPS*.

[41]See Renda, above, n. 30.

[42]L. Lessig, *Code and other Laws of Cyberspace* (Basic Books, 1999).

laws of cyberspace, opening up possible future legal forays into the technological environment in which users operate, for example by intervening to attribute jurisdiction and direction to smart contracts and realising, in the domain of enforcement, what Lessig once called the "perfect technology of justice".[43]

More specifically, GAIA-X includes both a policy working group, and an overall "architecture of standards" group, featuring European industrial players. The policy working group essentially works to translate the EU *acquis* into actionable inputs into the legal and semantic architecture of GAIA-X, whereas the architecture of standards matches policy actions with the development of technical specifications. Key EU policies embedded in GAIA-X include GDPR, the Cybersecurity Act, eIDAS, and the Data Strategy. Later in 2021, work on ensuring GDPR compliance by design and on interoperability obligations may pave the way towards the de facto imposition, via code, of the de jure obligations contained in key pieces of EU legislation.[44] GAIA-X is not reserved exclusively to European businesses, and indeed is already including large tech giants such as Microsoft and Google and Chinese companies like Huawei and Alibaba: but the extent to which these giants will be asked to adhere to rather strict, pro-competitive technical specifications (e.g., on data interoperability obligations) will determine whether GAIA-X will become, over time, an instrument of technological sovereignty as well as value redistribution, beyond what traditional public policies would be able to achieve.

In addition to these trends, it bears recalling another tendency that perhaps most clearly represents the change of course of EU digital policy. In the landscape painted by the European Commission, the era of open data, the age of the free flow of information that represented the most revolutionary banner of the Internet as a whole, will enter a phase of decline, at least in some provinces of cyberspace. A key element, in this context, is the new European data strategy, presented in February 2020 and already implemented through a first (indeed very timid) proposal for a Data Governance Act, which will be followed by other regulatory proposals, including a Data Act, in 2021.[45] In carving out separate data spaces, where real economy companies will be able to coordinate to optimise service provision and possibly retain the bulk of the value generated without surrendering (as has happened until now) to large cloud-based platforms, the Commission essentially responds to the need for a more assertive industrial policy: one that ensures that real economy firms in industrial markets do not end up witnessing the same value capture so far observed in consumer markets; and that as a consequence, the entire European industrial economy does not fall prey to the tech giants. The plea by EU Commissioner Thierry Breton, which aims at bringing Europe's share of the data economy up to the level of the continent's share of global GDP, is another important trace of this attempted coup.

Against this backdrop, a sneaky sensation emerges, possibly paving the way for a radical rethink of the battles fought, in good faith, over the past three decades. The era of open data is over, at least as far as industry is concerned. Net neutrality, an instinctively attractive principle, ended up becoming the main ally of the non-neutrality of platforms and of the unsustainability of the economy. The Schumpeterian winner-take-all competition, a promise of economic dynamism and prosperity, has become so undesirable that ordoliberal views have gradually regained citizenship after decades of silence and ostracism.[46] The idea of open innovation, praised as the promised land for smaller companies, has become a crime scene of contractual imbalances and value capture. More generally, the certainties of the early days of cyberspace, the most inspired ideological and libertarian battles, seem to have turned against the same people who supported them, and the same principles that inspired them. From here, to overcome the sneaky perils of the coming digital age, lawmakers will have to devise a new, more agile and hybrid toolbox, inspired by a combination of traditional law and "law as code".

[43]L. Lessig, 'The Zones of Cyberspace', (1996) 48 *Stanford Law Review*, 1403–1411.

[44]See GAIA-X: Policy Rules and Architecture of Standards, May 2020, available at https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-policy-rules-and-architecture-of-standards.pdf?__blob=publicationFile%26v=5.

[45]Proposal for a Regulation of the European Parliament and of the Council on European data governance, COM(2020) 767, 25 November 2020.

[46]O. Budzinski and A. Stöhr, 'Competition Policy Reform in Europe and Germany—Institutional Change in the Light of Digitization', Ilmenau Economics Discussion Papers, No. 117 (2018).

3 | WILL IT WORK? GAPS AND LOOPHOLES IN THE EU'S NEW DIGITAL STRATEGY

The post-pandemic recovery period will be, among other things, also an unprecedented testbed for the EU's ambition to govern cyberspace and set an example for the rest of the world. The new proposals for a regulation on Artificial Intelligence, the Digital Services Act and the Digital Markets Act, the various elements of the Data Strategy and the European Democracy Action Plan will be accompanied by the launch of an Important Project of Common European Interest on the edge/cloud architecture, the launch of data spaces in a variety of domains, as well as by the possible creation of a public–private partnership on Artificial Intelligence. In addition, the second half of 2021 will see the first concrete steps of the GAIA-X project, perhaps the most ambitious of the EU's attempts to restore sovereignty in cyberspace.

In this context, the European Commission seems determined to set a number of key indicators for the "digital decade", aimed at realising the objective of restoring digital sovereignty, as well as an ambitious new Digital Compass 2030 programme. The Commission, estimating that 90% of European data are managed by US companies, launched a consultation on selected targets to be met by the end of the decade, including the deployment of 10,000 climate-neutral highly secure edge nodes in the EU, "in a way that will guarantee access to data services with low latency (few milliseconds) wherever businesses are located"[47]; achieving a 20% share of the value of cutting-edge and sustainable semiconductors produced on a global scale; covering all European populated areas with 5G connectivity; adding 20 million employed ICT specialists in the EU; providing 80% of the population with advanced digital skills; achieving 100% coverage of online public services; and stepping up international cooperation with key strategic partners such as India, ASEAN and Latin America.

To achieve these goals, a number of challenges remain on the horizon, and the EU's ability to face them will determine whether the overall ambition of boosting Europe's data-driven economy will ultimately be met. Looking at the whole technology stack of the future Single Market, a number of nodes appear worthy of mention.[48] First, a more nuanced approach to connectivity will be required, since 5G technologies appear to be cost-effective only in a subset of use cases, with low-power alternatives and more decentralised architectures providing superior performance in many others.[49] Moreover, the ambition to provide user control over the flows of personally identifiable data must be backed by the deployment of "Personal Information Management Systems" (PIMS) such as those proposed by the Finnish innovation foundation Sitra, by the MyData movement, or by Tim Berners Lee's Solid project: however, at the time of writing no concrete prospects are emerging in this respect, and progress is needed, especially in light of the ongoing work on the review of GDPR.

Importantly, the governance of future data spaces, as well as their relationship with the emerging European Cloud Federation, appears to be obscure. On the one hand, while in some domains, such as health and automotive, bottom-up movements to propose solutions for the governance and sharing of data appear to be ongoing and promising, other sectors appear to still be at the starting line, and the governance arrangements that will enable future, constructive and pro-competitive data sharing are far from being clearly delineated. On the other hand, domain-specific groups in GAIA-X appear to be still insufficiently connected to the specific development in the data strategy. More generally, the link between the GAIA-X project and the European Cloud Federation appear to be still far from properly defined.

Furthermore, the EU ambition to conquer the edge/cloud space should be flanked and supported by a fully functioning Important Project of Common European Interest (IPCEI). This, already announced during 2020, is still in its infancy, and its governance is not yet known, let alone shaped. Similarly, a public–private partnership on Artificial

[47]See European Commission Communication, above, n. 25.

[48]See Renda, above, n. 30.

[49]See A. Renda, N. Reynolds, M. Laurer and G. Cohen, 'Digitising Agrifood: Pathways and Challenges', *CEPS monograph* (2019), available at https://www.ceps.eu/ceps-publications/digitising-agrifood/; M. Laurer and A. Renda, 'IOT4SDGs: What Can the Digital Transformation and IoT Achieve for Agenda 2030?', *CEPS Report* (2020).

Intelligence was announced, but has not yet been implemented. The content, funding and direction of these initiatives will be key to the success of future Single Market policies. In this respect, the regulation on Artificial Intelligence, proposed by the European Commission in April 2021, will certainly constitute an ambitious attempt to create a general framework for regulating AI, which has no precedents around the world. At the same time, the opportunities and risks associated with AI development will require much more than mere ex ante regulatory obligations on the side of the regulated entities, and much more than the currently envisaged system of conformity assessments. In particular, the AI regulation will create the need for innovative forms of governance, including the creation of agile institution mechanisms, able to monitor in real time whether high-risk AI applications are behaving in line with what is expected of them.

In a related domain, the regulation of digital platforms through the DSA and the DMA seems to be still floating between the expansion of competition policy tools, and the introduction of full-fledged new regulatory obligations. In addition, the enforcement of these new provisions seems to still be dependent on the ability of the European Commission to shoulder a massive new wave of complaints, as well as performing algorithmic inspections on platforms and, in particular, gatekeepers. Whether these rules will be enough to promote healthier competition in the digital ecosystem, it is difficult to say at the time of writing, but the search for a suitable balance between an exceptional set of rules within the realm of competition policy and a full-fledged sectoral regulation with rather harsh ex ante rules on a selected group of market players is not going to prove easy from the start.

Perhaps the most significant challenge ahead for EU institutions, in addition to getting enforcement right through a mix of technology-enabled and more traditional means, will be securing a high degree of policy coherence and convergence across the many initiatives launched over the past few months. These include, besides the ones mentioned in the past sections, also the new Industrial Strategy for Europe, which will be updated in April 2021; and the Next Generation EU programme, which will lead to unprecedented financial resources made available in the EU27 over the coming years, aiming for the "twin transition". On the horizon, a possible tension appears to be emerging between the overarching goals of the Green Deal and the Just Transition, the Commission's aspiration to become a more geopolitical actor pursuing sustainable development at a global level, and the possible push by Member States towards more aggressive interpretations of the digital sovereignty ambition, which would clash with the ideal of a more open approach to international cooperation (e.g., in AI or in the free flow of data with trust). The reconciliation of these goals in the future may require a proactive use of technology in support of a regulatory framework that, while levelling the playing field and remedying the inequalities that emerged during the first three decades of the Internet age, avoids falling into the trap of a ring-fenced, protectionist and inward-looking approach aimed at making the digital age fit for Europe, but perhaps unfit for Europeans and for the rest of the world.

ORCID


Andrea Renda https://orcid.org/0000-0002-9599-8234

How to cite this article: Renda A. Making the digital economy "fit for Europe". *Eur Law J*. 2021;1–10. https://doi.org/10.1111/eulj.12388