European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 113-124
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 09

Towards a New EU Regulatory Approach of the Digital Society *

Yves Poullet
(Emeritus Professor Faculty of Law, University of Namur, Co-chairman Namur Digital Institute)

ABSTRACT In recent times, the European Union has proactively multiplied the regulatory texts relating to various aspects of the digitalization of society. These texts take into account both the deep modifications of the digital market (merging of the telecommunications, audiovisual and information society services), the ubiquitous presence of certain actors and the increasing impact of our digital society not only on our way of doing business or conducting public affairs but also on our life and liberties. Through these texts, the Union's desire to chart a "Third Way" forward in terms of the development of our digital society, human centred, distinct from that of the United States and China and based in particular on respect for human rights . Beyond the multiplication of these texts, it is interesting to highlight a certain number of the characteristics of this EU regulatory approach: how the EU authorities have imposed a coregulatory model instead of self-regulation and how they are achieving a full consistent EU market. Furthermore, EU recent regulations adopt an asymmetrical approach in order to regulate especially the major actors and in order to ensure the proportionality of their intervention and the effectiveness of their regulations, the EU authorities promote a risk-based approach and of preventive measures, including the creation of internal compliance bodies, in addition to or instead of the traditional a posteriori legal control.

1. *Introduction*

The arrival of a new European Commission has resulted in a flurry of new regulatory texts in support of an increasingly proactive strategy to chart a third way for digital development. Artificial intelligence (AI for short), the *buzzword* of the advent of a digital society, has undoubtedly been the occasion for an intervention that goes far beyond the proposed AI regulation.

It is important to specify, first, this strategy that inspires Europe's regulatory action. At a time when regulatory projects are multiplying, the citizens of this Europe are wondering about the limits of this intervention by the European institutions. The issues of individual liberties, the attempts to democracy, the opening of our administrations, the health economy, the supervision of platforms, the regulation of new media against disinformation, etc. are all matters that the European regulator is concerned with.

A second point will detail the many facets of these projects, some of which are still open or simply envisaged.

The third point pinpoints the characteristics of digital texts in European legislation. The methods have changed. Gone are the days of directives and gone are the days of self-regulatory documents issued by the private sector. The European Union, including those advocating asymmetrical obligations about certain operators in the digital market, imposes detailed regulations. At the same time, there is a distrust of self-regulation and a concern for top-down co-regulation, which certainly leaves room for *soft law* but which is framed by numerous guidelines. A second feature is the creation and multiplication of administrative authorities at national level that are controlled or at least coordinated at European level. Anxious to ensure the proportionality of intervention and the effectiveness of regulations, we are seeing the emergence of a risk-based approach and of preventive measures, including the creation of internal compliance bodies, in addition to or instead of the traditional *a posteriori* legal control.

Finally, some reflections address the way in which the texts intend to ensure genuine European sovereignty, not hesitating to extend the application of these texts to companies located outside the territory of the European Union.

Before addressing these various points for the sake of completeness, I should have addressed the role of the Court of Justice of the European Union on the one hand, and of the Parliament, on the other, which is often a spur to the Commission's action. The multiplication of the Court's decisions is remarkable for its daring and innovative interpretation of regulatory texts, reinforcing them. The European Parliament's resolutions bear witness to the growing desire of this institution to play to the full its new assigned

* Article submitted to double-blind peer review.
The present text has been submitted in October 2022.

role of initiating and supporting the Commission's action. The limits of volume imposed on the present reflections constitute the only justification for our silence on their initiatives.

2. *The Objectives of a European Regulatory Policy for the Digital Society*

What specific regulatory response is Europe providing to the challenges of digital technology? Doesn't digital technology now stick to us, both figuratively and in reality? Does it not guide, for better or worse, our lives as well as those of companies and administrations? It is therefore important, and it is the role of the public authority, to map out the uses of a tool, which, increasingly, is the backbone of our economy, our society, our relationships, and ourselves. The introduction mentioned the European will to lead a third way. What is it about? This third way was undoubtedly prepared by the previous European Commission and the Parliament of the time, but it is now clearly affirmed by the famous "White Paper on Artificial Intelligence" published by the new Commission[1] and its President as soon as they took office. The strategy is explicitly stated in the White Paper and its implementation has since been carried out through texts that follow one another at an accelerated pace and go far beyond the issue of artificial intelligence.

As will be emphasised, it is a regulatory policy on data, its creation, use, transmission, and impact that Europe intends to develop in a coherent manner[2]). This is indeed a third way insofar as the European Union intends to conduct a digital development policy based on principles different from those that explain, on the one hand, the American policy which, no doubt wrongly, can be summarised as 'all for the market' and, more correctly, by the desire to maintain and develop the digital economy, on the one hand, by the desire to maintain and develop American leadership and, on the other hand, the Chinese policy marked - but we are probably close to a caricature - by State interventionism and an AI at the service of the economy, social governance by the State and the security of the latter to the detriment of the individual freedoms of citizens.

Europe intends to eliminate intra-European barriers to the deployment of AI and, more generally, digital technology. The clearly stated ambition is to enable the European Union "to compete with the massive investments made by third parties, notably the *United States*[3] and *China*".[4] [5]

The third path is based on the two terms used in the title of the White Paper on artificial intelligence: on the one hand, Excellence, which characterises the quality of applications and the research that supports their design, and on the other hand, Trust, which is necessary for the social acceptability of innovative digital developments, regardless of their field: education, health, mobility, public affairs, etc. It is a question of putting people at the centre of digital development and ensuring a solid framework for operators that allows for responsible innovation. Thus, "the Commission calls for a European society irrigated by digital solutions that are deeply rooted in our common values and that enrich the life of each one of us: citizens must have the possibility to develop themselves, to make choices in complete freedom and security, to

[1] European Commission, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM (2020) 65 final 8, Brussels, 18 February 2020.

[2] Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions, *A European strategy for data*, COM/2020/66, Brussels, 19 February 2020, final: "The European data strategy aims to make the EU a leader in a data-driven society. Creating a single market for data will allow it to flow freely within the EU and cross sectors for the benefit of businesses, researchers, and public administrations. People, businesses, and organizations should be empowered to make better decisions based on insights from non-personal data, which should be available to all".

[3] www.usinenouvelle.com/etats-unis.

[4] www.usinenouvelle.com/chine.

[5] One weakness, however, that is often complained about is the level of European investment. In this respect, the figures quoted by the JRC report (M. Craglia (ed.), *Artificial Intelligence - A European perspective*, Publications Office of the European Union, Brussels, 3 December 2018, https://doi.org/10.2760/11251): "... United States, investments by GAFAM (private sector) and public authorities, DARPA (US Department of Defence Research Directorate: 7.5 billion dollars in 2020); China, for a volume of more than 20 billion; Europe (2.5 billion euros for 2018-2020), following the joint declaration of the Member States in April 2018 on their cooperation in the field of artificial intelligence Note the figures given in the *White Paper on artificial intelligence* (op. cit, 4): "However, the amount of investment in research and innovation in Europe remains well below the public and private investment in this field in other regions of the world. Some €3.2 billion was invested in AI in Europe in 2016, compared to about €12.1 billion in North America and €6.5 billion in Asia".

engage in society, regardless of their age, gender, or professional background. Businesses need a framework that allows them to start, grow, share, and use data, innovate, and compete or cooperate on a level playing field. And Europe must have the choice to pursue digital transformation on its own terms".[6]

This policy, which is particularly explicit about AI systems, seeks to reconcile respect for European ethical values without concealing the fact that this respect has an economic objective: i.e., the creation of a strong and sovereign European market, in particular through the creation of European labels or certificates (see *below*). As Ms Vestager emphasised when presenting the proposal for an "AI Act" Regulation, the aim of this text is to implement the very principles of excellence and trust: "In the field of artificial intelligence, trust is not a luxury but an absolute necessity. By adopting these landmark rules, the EU is taking the lead in setting new global standards that will ensure that AI is trustworthy. By setting the standards, we can pave the way for ethical technology worldwide, while preserving the EU's competitiveness. Future-proof and innovation-friendly, our rules will apply when strictly necessary: when the safety and fundamental rights of EU citizens are at stake".

The purpose of this major document is, according to the Commissioner, fourfold:

1) Ensure that AI systems placed on the EU market and used are safe and respect existing fundamental rights legislation and EU values;
2) ensuring legal certainty to facilitate investment and innovation in AI;
3) strengthen the governance and effective implementation of existing legislation on fundamental rights and safety requirements for AI system;
4) facilitate the development of a single market for legal, safe and trustworthy AI applications, and prevent market fragmentation.

This policy cannot be achieved without perfect coherence of the actions of all the member countries and presupposes both the drafting of more and more precise and numerous texts and better and better compliance, including by foreign companies offering digital products or services on European "territory". It considers the merging of three previously clearly distinct worlds: that of electronic communications, that of the media and that of Internet services.

3. *Themes - Multiplying and Expanding*

The traditional themes are addressed by new texts, either updating or broadening the regulatory concerns. As far as *digital service operators and operations are* concerned, the 1999 "electronic signature" directive has given way to the eIDAS Regulation No. 910/2014 of 23 July 2014, which aims to establish a common basis for secure electronic interactions between citizens, businesses, and public authorities, by setting up a framework for electronic identification and trust services. The increased attention to consumer protection has justified various texts consisting of a "New Deal for Consumers" Directive 2019/2061 of 27 November 2019 for a better application and modernisation of consumer protection rules and Directive 2020/1828 of 25 November 2020 on representative actions to protect the collective interests of consumers.

Directive 2009/770 on certain aspects of contracts for the provision of digital content or services is also noteworthy. This directive aims to fully harmonise the rules governing the conformity of digital content or a digital service with the contract, remedies in the event of lack of conformity or failure to supply and the way such remedies may be exercised, as well as the modification of digital content or a digital service.

The issue of the *protection of individual liberties* refers to the adoption of the RGPD, in place of Directive 95/47. The enshrinement of the Charter of Fundamental Rights of the European Union, adopted on 12 December 2007, allowed for a firmer European approach, broadening the rights of the persons concerned at the same time as it was important to address new issues, in particular profiling.

It is known that the 2002 directive on data protection in the electronic communications sector, known as *e-Privacy*, which was amended in 2009, is currently being revised as a regulation to adapt it to the protection requirements linked to the emerging

[6] European Commission, *Communication from the Commission to the Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, *Shaping Europe's Digital Future,* COM(2020)67 final, Brussels, 1 February 2020, 2.

technologies of the Internet of Things and new communication services. Furthermore, the issue of access by law enforcement and judicial authorities to electronic evidence stored in the cloud awaits the adoption of the proposed Regulation on European orders for the production and preservation of electronic evidence in criminal matters.[7] In this respect, the European proposal, by forcing access to servers held by foreign companies, including in foreign territory, conflicts with the solutions of the American *Cloud Act* of 2018, which favours the law of the establishment of the operator of the *cloud* services, unless a treaty is concluded with the foreign country.

Freedom of expression and its abuses linked to violent or terrorist content of messages and disinformation, sometimes exacerbated by the pandemic, were the subject in May 2021 of "Guidelines" published by the Commission to reinforce the 2018[8] "Code of Practice on disinformation", but also of a proposal for a regulation, the "Digital Services Act", which proposes a regulatory framework for the provision of online services[9]. That proposal amends the famous provisions on liability of internet's hosting providers, contained within the directive on e-commerce dated from 2000, by extending the responsibility of information providers and overall, of platforms as regards the content disseminated through them.

The AVMS Directive 2018/1808 of 18 November 2018 determines, "taking into account *the evolution of market practices*", the minimum set of rules applicable in all EU Member States to audio-visual services including audio-visual product platforms and on-demand service operators. It promotes cultural diversity and regulates, inter alia, advertising, product placement, protection of minors, etc., and brings into the field of digital content regulation other authorities, namely the competent authorities.

It should be noted that this directive enshrines the disappearance of the social media or video-sharing services. It enshrines the principle of transparency of the operators of such services, regulates commercial communications and calls for appropriate national measures to protect young people and to combat violence and provocation to terrorism.

The fight against disinformation has been the subject of a "Guidance for strengthening the Code of practice on disinformation" and overall, the adoption of the *Digital Service Act,* Oct. the 19th of 2022. In addition, the fight against electronic terrorist messages was the subject of Regulation 2021/784 of 29 April 2021 on combating the dissemination of terrorist content online.

All these texts aim to "improve the functioning of the digital single market by enhancing legal certainty for hosting service providers and user confidence in the online environment, as well as guarantees for freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society, and media freedom and pluralism". They propose a control of the technological tools used to filter messages for their content or even to audit them, oblige at least some operators to set up human moderation and mediation bodies, and ultimately the possibility of recourse to the courts.

As for *intellectual property*, the same reference to technological developments justifies the adoption of Directive 2019/790 on copyright and related rights in the digital single market on 17 April 2019. The Directive "provides for rules to adapt certain exceptions and limitations to copyright and related rights to the digital and cross-border environment, as well as measures to facilitate certain licensing practices, including, but not limited to, the dissemination of commercially unavailable works and other subject-matter and the online availability of audio-visual works on video-on-demand platforms, with a view to ensuring wider access to content. It also contains rules

[7] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European orders for the production and preservation of electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council establishing harmonised rules on the appointment of legal representatives for the purpose of obtaining evidence in criminal matters*, n° 6946/19, Brussels, 28 February 2019.

[8] European Commission, *Guidance on Strengthening the Code of Practice on Disinformation*, COM(2021) 262 final, Brussels, 26 May 2021.

[9] On 15 December 2020, the European Commission presented its proposal for a regulation to regulate the digital single market: the *Digital Service Act*. This first proposal aims to provide a harmonised framework of rules for online services, mainly in terms of moderation of illegal content and transparency of service. This proposal distinguishes rules according to various categories of operators, from simple web services to very large platforms. See also, the Proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Ac), Brussels 16.09.2022, COM(2022) 457 final, still in discussion.

to facilitate the use of content which is in the public domain. In order to achieve an efficient and fair market for copyright, there should also be rules on rights in publications, on the use of works or other subject matter by online service providers who store and provide access to content uploaded by their users, on the transparency of 'authors and performers' contracts and on the remuneration of such authors and performers, as well as a mechanism for revoking rights which authors and performers have transferred on an exclusive basis".

Beyond this intervention in traditional areas, the European Union has addressed regulations to communication infrastructures, to the technology itself and to some of its products. About infrastructures, in terms of technology, cybersecurity has become a major issue in European policy. It is the subject of a Regulation 2019//881 of 17 April 2019 "on ENISA (European Union Agency for Cyber Security) and on Information and Communication Technologies Cybersecurity Certification".[10] With regard to products, without being exhaustive, it should be noted that the intelligent car is the subject of regulatory texts.

Regulation 2017/745, which the case law of the Court of Justice now extends to telemedicine software and AI applications in the health field, succeeded the Medical Devices Directive.

Then, finally, AI technologies, which are applicable in many areas, are the subject of a Commission proposal for a Regulation known as the "AI Act".[11] This proposal aims to provide a framework for the development of artificial intelligence applications, by distinguishing various categories based on an analysis of the risks associated with these applications. For so-called high-risk applications, it intends to establish both internal governance and a risk assessment procedure on the model of the Regulation on medical devices, including external evaluation by a supervisory authority including external assessment by a supervisory authority, maintenance of a register and European certificates of certificates of conformity. On the subject of robots, which often incorporate AI systems, the Commission is proposing, on the same day as its AI proposal, to replace the 2006 Machinery Directive by a new regulation on machinery and equipment[12] targeting notably robots, 3D printers, intelligent lawnmowers or cars. This new regulation will be better able to ensure integration of AI systems while reducing administrative burdens and costs through simplified through simplified procedures.

It should be added that the texts relating to AI refer to others that respond to the European strategy of creating a European data market and, at the same time, augur the possibility of setting up European *big data*, capable of feeding AI systems. As part of this policy of increased data circulation and sharing, the Commission has taken various initiatives. Recently, the Data Act[13] proposal intends to favour the data sharing as regards the data collected by Internet of things technologies, and that among all actors including the public sector, ensuring a functional interoperability between information systems, and excluding any "sui generis" right to the data base resulting from the collection of the data generated using the devices.

The main one is certainly the proposal for a regulation on European data governance (*Data Governance Act*) presented on 25 November 2020,[14] which encourages, through the creation of regulated services known as data sharing, the sharing of data not only between companies but also between the private and public sectors, and even between individuals and the public sector, with regard

[10] See, about 5G, NIS Cooperation Group, *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, CG Publication, 2020 and about connected cars, Consolidated text: Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, OJ L.151 14.6.2018,1 and ff. amended by the Commission delegated regulation 2021/1445, 23.06.2021, O.J. L. 313, 4 and ff.

[11] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence legislation and amending certain Union legislative acts* COM(2021*)*, Brussels, 21 April 2021, 206, final {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}.

[12] COM(2021) 202 final, Brussels, 21 April 2021.

[13] Proposal for a regulation on harmonized rules on fair access to and use of data, Brussels 23. 2. 2023, COM(2022)68 final.

[14] European Commission*, Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM(2020) 767 final, 2020/0340(COD), Brussels, 25 November 2020.

to "Data for public Good", within the framework of *data altruism*.

As far as the public sector is concerned, Europe is promoting the widest possible exploitation of public sector data by the private sector. In this respect, no sooner has the ink dried on the 2019 *Open Data* Directive,[15] which already significantly strengthens the obligations to make available information held by the public sector, than the proposed Data Governance Regulation of 25 November 2020[16] expands these obligations in one further aspect, namely, to open the re-use of protected data previously excluded from access.

Lastly, the European Union is paying particular attention to the regulatory framework for certain operators, the *very large platforms, which are* now described as the *gatekeepers* of the information society. In this respect, through their recommendation and profiling systems, they generate so-called 'systemic' risks, according to the definition given in the draft DSA, i.e. in addition to the impact on our individual freedoms; they also have an impact on the democratic functioning of our society and on social justice. The market share occupied by these companies and their strategy of diversification of activities profoundly de-structure the boundaries hitherto drawn by regulation between audio-visual services and digital services, such as functioning of the competitive market and oblige the European Union to intervene. This is the purpose of both the Regulation of 20 June 2019 "promoting fairness and transparency for business users of online intermediation services" and, more recently, the enactment of the *Digital Market Act*, which introduces asymmetric regulation of information service operators,[17] taking into account their importance on the market and therefore, their possibility to disturb a fair competition by giving advantages to their own subsidiaries or affiliates or by manipulating their customers by merging different data bases[18].

Furthermore, it should be noted that the Electronic Communications Code, since its revision in 2018,[19] now includes providers of so-called OTT (over-the-top) communication services, providers of instant messaging services, emails, telephone calls on the Internet and social networks, in the definition of electronic communications operators. They are therefore subject to the same obligations as "traditional" operators, in particular as regards interoperability, information and protection of end-users, public security and national defence, and even the financing of the universal service, and to specific rules on the protection of privacy.

Advanced technologies are indeed merging the previously separate markets of traditional electronic communications operators on the one hand and communications platforms such as What's App on the other. As noted in Recital 7 of the Directive, the convergence of the telecommunications, media and information technology sectors implies that all electronic communications networks and services should be subject as far as possible to a single European electronic communications code established by means of a single directive.

4. *Towards Original Modes of Regulation*

4.1. *Regulations instead of Directives*

What can we learn from this efflorescence of European texts? In what way do they mark an evolution in the European Union's modes of regulation? There are several points to be made in this respect: the first is the proliferation of regulations, whereas until recently Europe was content with directives. The example of the passage from the 1995 directive on data protection, which, according to the very terms of its recitals, left room for manoeuvre to the Member States, has given way to a regulation that not only imposes common rules but also creates the bodies for

[15] See Directive 2019/1024/EU of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, O.J.E., L 172, 20 June 2019, available online at: https://op.europa.eu/en/publication-detail/-/publication/a6ef4c41-97eb-11e9-9369-01aa75ed71a1/language-fr/format-PDFA2A. The proposal was adopted with minor amendments by the Committee on Industry, Research and Energy on 16 July 2021.

[16] COM (2020) 767 final.

[17] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Sept, the 14th, 2022. The Digital Markets Act introduces a new regulatory model based on a system of graduated obligations, known as "asymmetric", which adequately targets the largest players.

[18] The Data Act proposal (article 5.2) forbids that the "gatekeepers" shall be third party as regards the sharing of data generated by using IoT systems.

[19] Directive (EU) 2018/1972 of 11 December 2018. This directive replaces five directives.

maintaining and even amplifying this consistency.

No doubt there are still relays at national level (data protection and audio-visual control authorities, supervisory bodies for AI, etc.) whose powers of investigation and sanction have been strengthened, but these national authorities are forced to work in close cooperation and are even controlled by so-called European coordination bodies at European level.

4.2. *The proliferation of independent administrative authorities*

Several texts thus create European agencies or authorities responsible for ensuring the coherence of the actions of national authorities and for ensuring the uniform interpretation and application of texts. These authorities express themselves through "guidelines", recommendations, opinions, and reports and advise the Commission in its regulatory work. Without being exhaustive, let us mention: the EDPB in the field of data protection, ENISA in the field of cybersecurity, the Medical Devices Coordination Group, the European Artificial Intelligence Committee, the European Regulators Group for Audio-visual Media Services (ERGA), BEREC (Body of European Regulators for Electronic Communications) or in French, ORECE, which provides administrative and professional support to the European Commission.[20] AI and Data Act proposals are in the same way considering the setting up of national independent supervisory authorities.

With the same concern and to further increase the effectiveness of the regulatory texts and ensure their rapid adaptation to the needs of technological development, the texts also confer powers on the Commission, either to monitor the application of the regulations in the form of reports in particular, or to adopt delegated acts pursuant to the text of the Regulation. Thus, to take the examples of the "AI Act": reviewing the scope of the AI Regulation, completing the list of high-risk systems, etc.

It should be noted that when the Commission is directly responsible for implementing the provisions of a European competence such as, in competition, the texts adopted in these areas such as the DMA, the Commission, assisted by an Advisory Committee on Digital Markets made up of representatives of the various member countries, can directly impose binding measures on companies.

The proliferation of administrative authorities created by all these recent texts raises difficulties when it comes to analysing the impact of a technology in a cross-cutting manner or to giving a ruling in a dispute that involves the various issues considered separately in the regulatory framework and by bodies with different cultures and prerogatives. To take the example of the use of recommendation and profiling systems by digital platforms, this is an issue that touches on data protection, freedom of expression and media regulation, competition, and consumer protection.[21]

This need for a cross-cutting approach can, in our opinion, only be met by clarifying the role and competences of each category of administrative authorities but, above all, by institutionalising the creation of forums for dialogue between these different bodies, without which there is a risk of contradictory interventions or even rivalry between authorities.

It is worth noting, in connection with the designation of the proposed national supervisory bodies for AI, that data protection authorities have asked to assume this competence, even though data protection issues are only part of the risks to be considered when assessing AI systems. This is

[20] "BEREC aims at fostering the independent, consistent and high-quality regulation of digital markets for the benefit of Europe and its citizens". (BEREC strategy 2021-2025). Directive (EU) 2018/1972 of 11 December 2018 confers a significant number of new tasks on BEREC "such as issuing guidelines on several topics, reporting on technical matters, keeping registers, lists or databases and delivering opinions on internal market procedures for draft national measures on market regulation. Overall, the EECC aims to create an internal market for electronic communications within the EU while ensuring a high level of investment, innovation, and consumer protection through enhanced competition". National regulatory authorities and the Commission should take the utmost account of the recommendations, guidelines and best practices adopted by BEREC (Recital 21 of the Electronic Communications Services Directive). BEREC works to ensure that European legislation is applied in a uniform manner, so as to enable the EU to have an effective single market in electronic communications. It provides advice, on request and on its own initiative, to the EU institutions. It consists of a Board of Regulators. This is a body composed of the heads (or high-level representatives) of each national regulatory authority.

[21] Another example is the regulation of connected cars, which involves questions of infrastructure choice (5G or WiFi), data protection, interoperability, and security standards.

probably one of the first initiatives to regulate a technology across the board. An example to follow?

4.3 *Coregulation under control*

Finally, it is emphasised that the convergence of previously distinct sectors such as the worlds of telecommunications, audio-visual and e-commerce services now requires online platforms in particular to juggle regulations from different cultures, which are applied cumulatively and, it is hoped, coherently in their own right. Europe's desire to achieve its objectives explains the regulatory approach and its mistrust of self-regulation, which is difficult to control and above all the prerogative of the powerful. This attitude is not in contradiction with the forms of co-regulation that we have described in previous texts as top-down, i.e. private regulatory mechanisms are certainly promoted but severely framed by a regulation that sets the guidelines and even controlled by the independent administrative authorities set up and even by the Commission itself.[22]

This trend is reflected in many texts and, sometimes, explicitly, as in these recitals (See recitals 12 and 14 translated by Article 4a) of the Audio-visual Services Directive: "Member States should, in accordance with their different legal traditions, recognise the role that effective self-regulation can play as a complement to existing legislative, judicial and administrative mechanisms, as well as the usefulness of its contribution to the achievement of the objectives of Directive 2010/13/EU. However, while self-regulation can be a complementary method of implementing certain provisions of Directive 2010/13/EU, it should not be allowed to replace the obligations of the national legislator. Co-regulation, in its simplest form, provides a legal link between self-regulation and the national legislator, while respecting the legal traditions of the Member States. In co-regulation, the role of regulator is shared between the stakeholders and the public authorities or national regulatory authorities and bodies. The role of the competent public authorities includes the recognition of the co-regulatory system, the audit of its procedures and its financing. The possibility of state intervention should exist, within the framework of co-regulation, when the objectives of the system are not met…". It is illustrated by the way in which, as regards disinformation, after having accepted in 2018 self-regulation by the major market players, in addition to the launch of the DSA proposal already studied, the Commission published on 26 May 2021 - the title is evocative - the "Guidelines for strengthening the Code of Conduct on misinformation".[23]

Without being exhaustive, we can mention in the same vein the articles 40 et seq. of the GDPR, which, while recognising various methods of private regulation (codes of conduct, labels, certificates), set minimum conditions for them and provide for their approval by DPAs.[24] The "AI Act" allows for self-regulation but only for low-risk AI applications. It should be noted that the European authorities insist on *multi-stakeholder* participation in the drafting of self-regulatory instruments.[25]

It should be added that this same concern to bring private regulation into line with the requirements of public regulation is also expressed in relation to another mode of regulation: technology, the operation of which imposes what many authors (see Reidenberg, Trudel or Lessig) have called the *lex informatica or electronica*. It is important that the *design of* technological tools and their applications conform to the rule of law from the outset. A number of European texts require designers or users to comply with the

[22] For a fuller account of the relationship between European regulation, self-regulation and the "lex informatica", see Y. Poullet, *Vues de Bruxelles. Modes alternatifs de régulation et libertés dans la société du numérique*, in C. Castets-Renard, V. Ndior et L. Rass-Masson (eds.), *Enjeux internationaux des activités numériques*, Brussels, Larcier, 2020, 91-137.

[23] "The Guidance aims at evolving the existing Code of Practice towards a co-regulatory instrument foreseen under the Digital Services Act (DSA), offering an early opportunity to design appropriate measures to address systemic risks related to disinformation stemming from the functioning and use made of the platforms services in view of the anticipated DSA risk assessment and mitigation framework".

[24] On this point, the policy followed by DPAs, *Guidelines 1/2019 on codes of conduct and monitoring bodies under Regulation (EU) 2016/679*, 4 June 2019.

[25] Among many examples, we can cite the injunction on 2 of the "Guidance for strengthening the code of Practice on disinformation": "Online platforms and all other players of the online advertising ecosystem should thus take responsibility and work together to defund disinformation. (See, in particular, the creation by the 'Guidances' of the European Digital Media Observatory, which includes researchers, representatives of 'fast-checkers' and other 'relevant stakeholders".

law: for example, the GDPR puts forward the principle of "privacy by design" (Article 25); the 2018 Copyright Directive insists that the control systems used to combat illicit copying respect the law's exceptions (Article 17.7); the DSA proposal (Article 28) requires the verification of recommendation systems and we will come back to the "AI Act" proposal which, beyond the "Privacy by design" of the GDPR, advocates "Ethical values by design".[26]

4.4. *Asymmetrical regulation of the players*

Another characteristic seems to be emerging in the most recent European Union texts, namely asymmetrical regulation of both the players and the applications operated, or products or services offered by them, depending on the risks (*risk-based approach*) associated with these applications, products or services. In both cases, the regulatory asymmetry is justified by the principle of proportionality, affirmed by Article 5(4) of the Treaty on European Union, which stipulates that the Union must not in exercising its powers do more than is necessary to achieve its objectives. Let us look at these two points in more detail.

Some European regulations impose heavier obligations on certain categories of actors. For others, they grant exceptions to facilitate their development. The second chapter (*supra,* no 10) already pointed to certain provisions imposed on communication and information platforms, such as the equal and transparent treatment of professional users by these necessary intermediaries. Similarly, the DSA imposed obligations on *very large platforms* (i.e. those with a customer base equal to or greater than 10% of the European population) to monitor content and audit recommendation systems.

At the other end of the spectrum, there is a desire to protect research organisations, start-ups and even SMEs in order to guarantee innovation. Thus, Articles 3 and 4 of the 2019 directive on the protection of intellectual property provide scientific research bodies with the exceptional right to carry out data searches, notwithstanding the sui generis or intellectual property rights of right holders or their successors. The same concern can be found in the texts relating to access to public data and data sharing. Similarly, Article 55 of the *IA Act* provides for the possibility of national measures "in favour of small providers and users".

It is known that the 2019 European Regulation promoting fairness and transparency for businesses using online intermediation services is fully justified by this desire to protect SMEs[27] and that the intermediation services envisaged under the *Governance Data Act* proposal are intended to assist SMEs to benefit from the advantages of data sharing. More recently, the Data Act proposal is protecting under the common concept of "user" both individuals and legal persons by affording the same data protection including the rights to access, to be informed and to consent to the sharing of the data generated by their use of IoT devices.

Finally, Article 17.6 of the 2019 Copyright Directive exempts from certain due diligence obligations "new providers of online content sharing services whose services have been publicly available in the Union for less than three years and which have an annual turnover of less than EUR 10 million calculated in accordance with Commission Recommendation 2003/361/EC (which defines SMEs)".[28]

4.5. *The 'risk approach'*

The genuine risk-based approach leads to the creation of new obligations when certain criteria proposed by the regulation indicate

[26] In addition to compliance with the Law, the European Commission's May 2019 statement, following the recommendations of the expert group, AI applications should not only be consistent with the Law but also adhere to ethical principles.

[27] "Online intermediation services can be critical to the commercial success of businesses that use them to connect with consumers. To take full advantage of the online platform economy, it is therefore important that businesses can rely on the online intermediation services with which they enter a commercial relationship. This is important mainly because the increasing intermediation of transactions through online intermediation services, because of significant indirect data-based network effects, leads to an increased dependence of these user enterprises, in particular micro, small and medium-sized enterprises (hereinafter referred to as "SMEs"), on these services to contact consumers" (Recital 2).

[28] In paragraph 2 of the same article, a second criterion is added to qualify the application of the first: "Where the average number of unique visitors per month of such service providers exceeds 5 million, calculated on the basis of the previous calendar year, they shall also be required to demonstrate that they have used their best efforts to avoid further uploads of the works and other protected subject matter covered by the notification for which the rightsholders have provided the relevant and necessary information".

that higher risks are present. This approach is already used, but in a very limited way, in the provisions of the GDPR: Article 35 reserves the obligation to carry out an impact assessment only to processing operations presenting a "high risk" to the rights and freedoms of natural persons. The notion of "high risk" remains unclear. The Regulation on medical devices similarly distinguishes between different classes of products and services according to the purpose of their use and the risks related to health and safety, and subjects "high risk" classes of products to conformity assessment procedures.

The same idea runs through the "AI ACT". The proposal sets out the prohibition of illegal practices of artificial intelligence[29] (Art. 5); it establishes a system of control and management of high-risk AI systems (Art. 6.2) listed in an annex that may be amended by the Commission; it imposes specific obligations for lack of transparency on certain hidden applications "in particular when ultra-realistic dialogue or video tricks are used"; and, finally, it leaves other applications presenting a minimal risk to the self-regulation of the market. The "AI Act", or rather the work of the *High-Level Group of Experts on AI* on the ethics of AI,[30] to which this proposal constantly refers, broadens the risks to be taken into consideration when assessing AI applications. Thus, in addition to the risks to our individual freedoms, there is the need to take into consideration the so-called collective risks specific to a group of people or not, the risks of undermining social justice and, beyond that, the societal risks, such as those to the environment, democracy, and respect for the rule of law. This broadening is reflected in the definition of "systemic risks" linked to the operation of rating and recommendation systems and their use by "very large platforms".[31] We know that the first works on the liability of AI systems[32] retain the same idea of differentiating the responsibilities of the "producers" or professional users of AI systems according to the seriousness of the damage that the use of the systems may cause.

Another consequence of the risk-based approach is that it fully justifies the shift from a classic legal drafting - based on the definition of behavioural content to be respected and, in the event of non-compliance, on the repression or *a posteriori* sanctioning of breaches of the regulations - to an *a priori* approach based on the obligation to assess risks, i.e. to set up a risk assessment procedure and monitor compliance with this procedure. The preventive risk-based approach seems to be a characteristic of recent European regulations. The example already cited of the "Privacy Impact Assessment", introduced by the GDPR, thus shifts the scope of intervention of the regulation towards a preventive approach of risk avoidance by the need to set up an assessment procedure at the design stage of the processing. The same idea runs through the other regulations mentioned in the previous paragraph. In particular, the proposed "IA Act" develops this procedure at leisure, defining its stages, its content, insisting on the participation of all the interested parties, etc. This approach is to be commended, although it is administratively more cumbersome and can only be justified in cases of significant risk.

4.6. *Towards more effective regulations*

Chapter 1 emphasised *in fine* the Union's concern to ensure the effectiveness of

[29] For example, subliminal message manipulation systems, the exploitation of vulnerabilities, the use by the public sector of "social ranking" systems leading to potential discrimination between individuals or groups, biometric systems operating in real time and remotely, placed in public places (e.g. facial recognition systems).

[30] High-Level Expert Group on AI (HLGE), *Ethical guidelines for trustworthy AI*, 8 April 2019, No. 67, text available at: Ethics guidelines for trustworthy AI - Publications Office of the EU (europa.eu).

[31] Recital 57 of the DSA describes these so-called risks. The first concerns the extent to which online platforms with a significant market share can disseminate illegal content. The second concerns "the impact of the service on the exercise of fundamental rights, as protected by the Charter of Fundamental Rights, including freedom of expression and information, the right to privacy, the right to non-discrimination and the rights of the child. Such risks may arise, for example, from the design of the algorithmic systems used by the very large online platform or from the misuse of its services through the submission of abusive notifications or other methods aimed at preventing freedom of expression or hindering competition". The third risk is the use of mechanisms put in place by the platform, such as the recommendation system, to manipulate others in elections, to spread intentionally wrong messages that endanger public health, democracy, etc.

[32] European Commission, *Liability for Artificial Intelligence and other emerging digital technologies*, Report of the Expert Group on Liability and New Technologies, Section on New Technologies, Brussels, 21 November 2019. The European Commission seems to want to take up the ideas of this proposal for a regulation through a profound modification of the 1985 Directive on liability for defective products.

regulation, i.e. to guarantee compliance. The preceding paragraphs have already illustrated the way in which the Union intends to respond to this concern, by bringing self-regulation into line, by translating regulatory prescriptions into technology, by the role of the administrative authorities, not forgetting regular monitoring by the European Commission. One point must be added: the imposition of internal *compliance* mechanisms. The GDPR imposes (Article 37 et seq.) the obligation for certain companies to appoint a data protection officer, who enjoys a status that ensures a certain protection and has numerous competences and missions to ensure compliance with the GDPR. Other texts have since joined this idea. Thus, the so-called DSA proposal obliges, on the one hand, platforms to set up internal complaint handling systems, responsible for ensuring the legality of decisions taken automatically or not by the platform and, on the other hand, very large platforms to appoint one or more compliance officers.[33] Article 15 of the Medical Devices Regulations 2017 provides that "manufacturers shall have at least one compliance officer within their organisation with the requisite expertise in the field of medical devices".

4.7. *The EU "sovereignty" in the global digital space*

Finally, we shall mention the European determination to fully exercise its sovereignty in the digital space, not by creating technical gateways as notably Russia and China but by using the legislative tools and by ensuring their full effectiveness. This sovereignty implies, on the one hand, the extension of European rules to companies located outside Europe but also, on the other hand, the presence on the European market of products or services that comply with these regulations. The first facet of this sovereignty, i.e "control of our destiny on the computer networks",[34] is the trust and values of the European Union.[35] The trust and values of the European Union, which are reflected in the regulatory texts, can only be guaranteed and respected to the extent that, in a global digital market, the services and products using artificial intelligence and deployed on European territory effectively comply with the requirements of European regulations. It is on the basis of this premise that, in particular, the GDPR (art. 3) and the proposed regulation on AI or digital services do not hesitate to extend their scope of application to companies located outside the European Union when the processing, AI application or digital service is aimed at a clientele located in the European Union or when the application or product is intended for the European[36] market or residents. This broadening of the scope *ratione loci* of the European texts reflects the European will to use the regulatory tool to guarantee the protection of persons residing in Europe and, consequently, their trust in the AI tool developed or used there. Beyond that, it is an attempt to export the European regulatory model, insofar as the penetration of the European space by companies located outside Europe obliges them to obey the rules that prevail there and invites them to avail themselves of the added value of these rules with regard to all their markets. The same idea of sovereignty is reflected in the proposed "e-evidence Act", which allows police and judicial authorities to request data stored

[33] Article 32.2: "Very large online platforms shall only appoint, as compliance officers, persons who have the professional qualifications, knowledge, experience and skills necessary to carry out the tasks referred to in paragraph…".

[34] www.lepoint.fr/politique/emmanuel-berretta/la-souverainete-numerique-ce-dossier-qui-effraie-hollande-et-valls-13-01-2016-2009389_1897.php.

[35] On digital sovereignty, read, among others, the excellent contribution of A.T. Norodom, *Être ou ne pas être souverain, en droit, à l'ère numérique*, in *Enjeux internationaux des activités numériques*, C. Castets-Renard, V. Ndior et L. Rass-Masson (eds.), Brussels, Larcier, 2020, 21 and ff.

[36] The argument is noted in several regulations and proposed regulations, such as the RGPD, the AI proposals, the DSA... Among all these texts, let us simply quote: "As online intermediation services and search engines have a global dimension, this Regulation should apply to providers of such services, whether they are established in a Member State or outside the Union, provided that two cumulative conditions are met. The first is that business users or users of business websites should be established in the Union. The second is that the business users or users of business websites should offer, through the provision of these services, their goods or services to consumers located in the Union for at least part of the transaction. In order to determine whether business users or users of business websites offer goods or services to consumers located in the Union, it is necessary to determine whether it is obvious that business users or users of business websites direct their activities towards consumers located in one or more Member States" (Explanatory Memorandum, point 9 of the Regulation of the European Parliament and of the Council promoting fairness and transparency for business users of online intermediation services, adopted on 14 June 2019 (OJEU, L.186, 11 July 2019, 57-79).

outside Europe from companies based outside Europe when fighting certain serious crimes.
The requirement of sovereignty also implies, as a second facet of the Union's sovereignty over the digital space, the promotion of products or services that comply with European requirements. Indirectly, the measure aims to encourage the development of a digital products and services industry. Several texts thus set up European certificates which allow companies that use them to be presumed to meet the regulatory requirements and citizens to have a reassuring quality label. The GDPR provides for this possibility in the context of co-regulation. An EU Trust Mark is established for certification trust service operators under the eIDAS Regulation. The 2019 Cybersecurity Regulation establishes a system of voluntary certification to ENISA of products, services or procedures related to their security under certification schemes adopted by the Commission.[37] The regulations on medical devices and on AI represent a step forward in this area insofar as, including for foreign importers, they prescribe, at least for systems or devices presenting a higher risk, this obligation to be certified internally or, exceptionally, by an approved notification body, organise the quality control of the certification by a supervisory body and, finally, organise a European register of such certificates. These certification systems are a major challenge for the creation of a European market for products and services that comply with regulatory requirements and the promotion of European players on this market, with the hope that these certificates can also be an added value on export markets.

[37] See Articles 46 *et seq.* of the Regulation of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on cybersecurity certification of information and communication technologies: "1 The European Cybersecurity Certification Framework is hereby established in order to improve the conditions for the functioning of the internal market by enhancing the level of cybersecurity within the Union and by providing a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes. 2 The European Cybersecurity Certification Framework shall provide a mechanism to establish European cybersecurity certification schemes and to attest that ICT products, ICT services and ICT processes that have been assessed in accordance with these schemes meet defined security requirements, with the aim of protecting the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or the functions or services that are offered by or accessible through these products, services and processes throughout their life cycle".

5. *Conclusion*

Our contribution aims to highlight this pervasiveness of European regulation. The erasure of borders due to the creation of a universal digital space does not mean the free pass that the Net superpowers dream to impose their own regulation through self-regulation and more insidiously by technological options. The European Union does not intend to reinstall the barriers or, at least, the filters that certain powers such as China or Russia surround their national spaces with, but at least to subject the entry into the lives of European citizens, companies and administrations to a certain number of precautions which, as we have seen, go well beyond the sole concern of data protection and individual freedoms to extend to the protection of our European democratic societies and the values of social justice. In the name of these values, it is asserting and even imposing - some would say imperialistically - its regulatory choices and leaving behind the defensive culture that has often been its own. To do this, it puts a damper on the principle of subsidiarity and refuses the profusion of national texts whose impact would have been insufficient to combat the dangers of an area which would otherwise have obeyed the law of the strongest or the 'lowest bidder' country. The challenge of "excellence and trust" can only be met together. To this end, the Union is adopting texts that are undoubtedly far removed from traditional approaches; it is multiplying the links between law and technology to ensure compliance with the former; it is forcing certain cultures, such as that of property by encouraging data sharing, that of an administration that is jealous of its secrets and its data, and that of administrative authorities that are jealous of their traditional competences and prerogatives.
The regulation of the Union of our digital society opens vast areas for us lawyers and, no doubt, new ways of doing things for a better society.