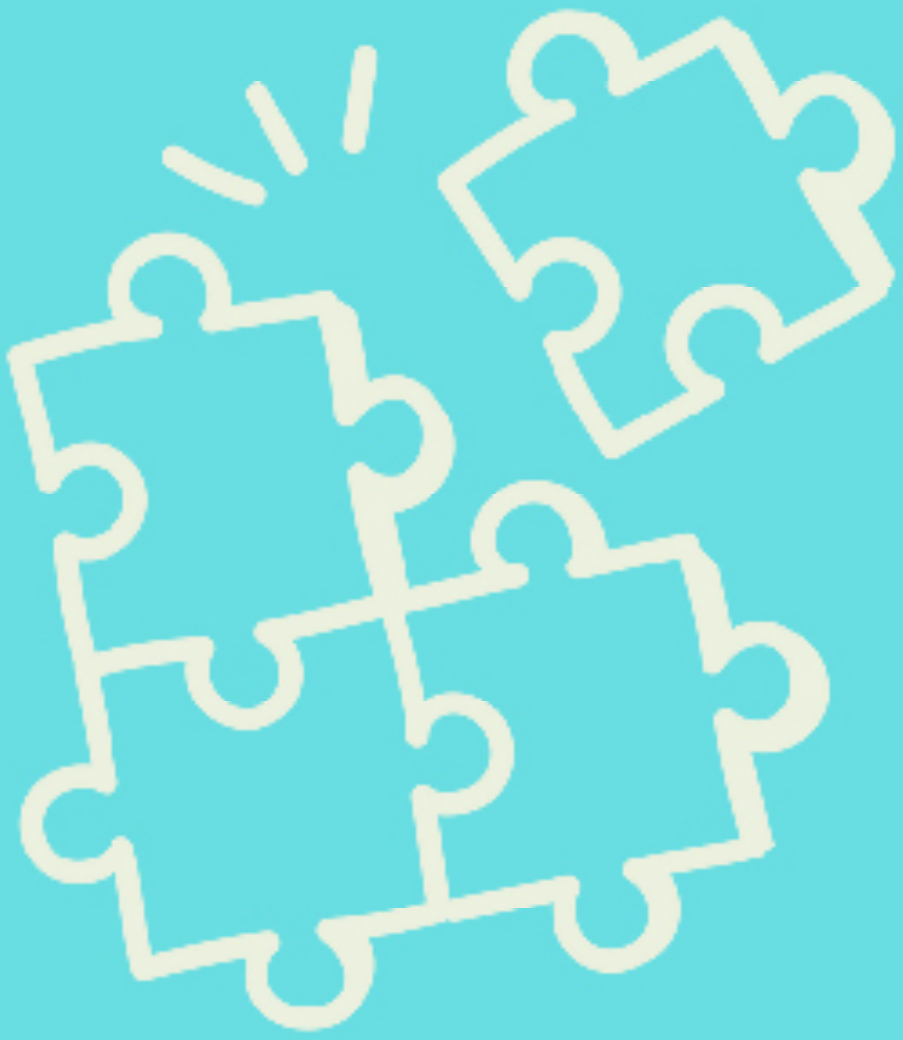
Renaissance Numérique



NOTE NOVEMBER 2024

EU Digital Policy: the Time Has Come to Connect the Dots

Table of contents

A digital policy lacking overall vision

In the tumult of our societies' digital transformation, the last five years of activity by the European Parliament and Commission have been marked by a succession of regulations[1] in the wake of the General Data Protection Regulation (GDPR)[2] coming into force in 2020. As a result, the stack of parallel legislation affecting digital[3] [4] now suggests a legal landscape that is as complex as it is fragmented.

There is no doubt that each piece of the European legislative puzzle had its sectoral or systemic *raison d'être*. Thus, there's no need to question the legitimate motivations behind each piece of legislation. They are public, they deserved to be supported, they were debated and then arbitrated with respect for political institutions and their underlying missions.

When it comes to architecture, as with regulation, a building is only as strong as the elements that make it up. A pile of stones doesn't make a building without an overall vision and cross-disciplinary governance. This vision, in architecture as in design in general, is not the sum of the objects we juxtapose, but the space left by their juxtaposition. In terms of regulation, as in architecture, it's not enough for the foundations to be laid and the building to be above water, for it to be habitable.

Once the law has been passed, decrees and guidelines are needed to specify the details of the text and to organize coordination with pre-existing standards. And therein lies the rub: while it has not taken the time to put the finishing touches to recently adopted texts, the European Commission seems to have already moved on to the next legislative project. This at a time when conflicts between regulators are appearing and adding to conflicts between standards, giving rise to contradictory injunctions, each of which is accompanied by sanctions and a judge, but with no arbitration rules other than jurisdictional and repressive.

The deleterious consequences of this unfinished regulatory profusion are beginning to be felt, foreshadowing difficulties in implementing and coordinating the texts adopted in recent years.

---

[1] Bruegel, "Overview of EU Legislations in the Digital Sector", November 2023: https://www.bruegel.org/sites/default/files/private/2023-11/Bruegel_factsheet.pdf

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

[3] "Regulatory pause in tech? Not with all these European texts to be reopened", *Contexte*, June 7, 2024: https://www.contexte.com/article/tech/les-clauses-de-rendez-vous-deja-connues_188238.html

[4] IAAP, Organizational Digital Governance Report 2024 p. 17: https://iapp.org/media/pdf/resource_center/organizational_digital_governance_report.pdf

Companies and public bodies are sometimes at a loss, faced with a myriad of laws whose applicability and compliance have become a challenge (not least because of their financial cost, especially for smaller companies[5]). What's more, the identification of the competent regulator is becoming increasingly plural, and arbitration between the various texts is more a matter of hope than an established mechanism.

The genesis of a legislative shrouding

Before 2020

Regulatory activity in recent years has been dominated by work on two major pieces of legislation.

On the one hand, the GDPR adopted on April 27, 2016 after four years of intense debate, has been the subject of more draft amendments than there were during 25 years of construction of the Common Agricultural Policy. Coming into force on May 25, 2018, it replaced Directive 95/46 of October 24, 1995[6] , which until then had been the common European foundation for the protection and movement of personal data. The GDPR promised European citizens and the rest of the world a common, homogeneous vision and interpretation of data protection as envisaged by the values of the European Union.

On the other hand, the draft e-Privacy Regulation[7], which has been at a standstill for seven years due to divergences between member states, is intended to establish specific rules for the provision and use of electronic communications services – in short, the internet in general. This draft regulation was intended to update Directive 2002/58/EC, known as the e-Privacy Directive[8] , once the GDPR has been newly adopted. In November 2024, it is still a long time coming, leaving gaps in interpretation to a set of regulators who are not always those of the GDPR, or who have no obligation to agree on common interpretations of today's core challenges: geolocation, targeted advertising, traffic data processing, e-mail marketing, and so on.

---

[5] An impact assessment produced by the European Commission as part of the AI Act shows that, for a company with 50 employees, bringing a single AI-enabled product to market could result in compliance costs ranging from 216,000 to 319,000 euros. European Commission (2021), "Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe", Final Report (D5): https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31995L0046

[7] Regulation on privacy and personal data protection in electronic communications and repealing Directive 2002/58/EC: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52017PC0010

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32002L0058

In parallel with the gradual adoption of these two major texts, Thierry Breton, the European Commissioner in charge of the internal market from 2019 to 2024, has orchestrated a vast legislative movement aimed sometimes at supplementing existing regulations, sometimes at adopting new ones, thus adding layers of regulation in fields that are constantly evolving.

Since 2020

Since 2020, two major sets of legislation have been enacted. The first updates existing legislation, reinforcing or redistributing the powers of existing regulators. This is the case, for example, with the new powers – notably of sanction – granted in France to the 'ANSSI'[9] by the 'NIS 2' Directive[10]. The second series of texts concerns new regulations with no dedicated regulators, leaving Member States to implement and interpret these texts according to national dynamics, increasing the powers of certain regulators, depriving others of some of their prerogatives, or creating new entrants in this booming market of digital regulations.

We owe this plasticity to the program launched in 2019 by Thierry Breton, the *Digital Decade 2020-2030*, or "Europe's digital decade"[11] , which set out the main lines of digital development. Traditionally, such announcements define the legislative mandate of each new Commission, following the European Parliament elections. In this case, Thierry Breton took care to avoid linking together the major principles and previous texts, in order to avoid political and institutional blockages. By tackling a variety of issues at the same time, the European Commission was able to postpone the "battle of leaders" between complementary or antagonistic regulators – in charge of personal data and individual freedoms, media and content, protection of consumers and minors, competition, cybersecurity, operational resilience, platforms and systemic players, artificial intelligence, technological sovereignty, etc. – until the implementation stage.

For example, it's common to hear people talk about the "DMA/DSA" pair[12] even though they don't have the same scope of application. Or to combine the Digital Governance Act

---

[9] Renaissance Numérique, "7 recommandations sur le projet de loi de transposition de la Directive NIS2", April 2024: https://www.renaissancenumerique.org/publications/directive-nis2

[10] Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022 on measures to ensure a high common level of cybersecurity in the Union, known as "NIS2", is the revision of the 2016 NIS Directive. It aims to harmonize cybersecurity requirements for member states and businesses, taking into account new challenges in the field of network and information system security.

[11] European Commission, Europe's Digital Decade: digital targets for 2030: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

[12] European Commission, Sneak preview: how the Commission will apply the DSA and DMA - Blog of Commissioner Thierry Breton: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_4327

and the Data Act to address them in their entirety, as two convergent regulatory instruments. And to use concepts in different contexts to map out new avenues of regulation, as is the case with the notion of *"very large online platform*" taken from the DSA, which is sometimes taken up in the context of freedom of consent within the meaning of the GDPR.

All this raises the question of regulatory coordination and overview in the event of conflicting standards.

Four main sectors subject to specific regulations

Platforms and intermediation services

- The Digital Markets Act (DMA) Regulation[13] of September 14, 2022, aims to combat the anti-competitive practices of digital giants and correct the imbalances of their domination of the European market, while strengthening the protection of online users. Gradually applicable since May 2, 2023, it came fully into force on March 6, 2024, the date from which the digital giants must comply with new obligations and prohibitions or face heavy fines.
- The Digital Services Act[14] of October 19, 2022, sets out the principle that what is illegal offline is illegal online. It lays down a set of rules to make digital platforms more responsible in the fight against the distribution of illicit or harmful content or illegal products (child pornography, racism or hate speech, false information, sale of drugs or counterfeit goods).

The European data strategy[15]

- The Data Governance Act[16] , applicable from September 24, 2024, aims to guarantee access to large volumes of data for the benefit of the European economy. It also organizes controls to preserve the European Union's digital

[13] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on fair and contestable contracts in the digital sector: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925

[14] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a single market for digital services and amending Directive 2000/31/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

[15] European Commission, "European Data Strategy": https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_fr

[16] Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

sovereignty. In addition, this regulation enables open access to data to be articulated with the GDPR.

- The Data Act[17] will apply from September 12, 2025. This text aims to encourage greater openness of data from the Internet of Things, in order to stimulate the development of a competitive data economy, beneficial to both users and European businesses.

Finally, there are plans to create common European data spaces specific to certain domains, starting with a European Health Data Space (EHDS).

Artificial intelligence

The Artificial Intelligence Regulation[18] (AI Act), ambitions to ensure that AI systems used within the EU are reliable and respect the fundamental rights and values of the EU. To achieve this purpose, the text focuses on the transparency, accountability and safety of AI systems. The AI Liability Directive[19] , proposed on the same day as the AI Act, aims to define homogeneous civil liability rules applicable to artificial intelligence systems, in order to guarantee the safety and protection of European citizens' rights.

EU policymakers have welcomed the rapid timetable for adoption of the AI Regulation, showing that the EU is at the forefront of regulation. However, the time taken to organize this regulation and its interpretation in a coherent way will be very long, for several structural reasons.

Firstly, each member state will appoint its AI regulator, either a new one or an existing one. During the first few years of the AI Act's application, each will also have to arbitrate – or allow to persist – conflicts of competence between regulators (personal data protection, cybersecurity, competition and consumer protection) and with the judicial authorities, who will have the task of implementing a European civil liability mechanism – which has yet to be defined.

Secondly, this division into two texts, (i) governing principles and obligations but not regulators on the one hand, and (ii) a harmonized civil liability regime within the European Union, on the other, may only become clear after a multitude of rulings by the Court of Justice of the European Union, i.e. not for a few years yet.

[17] Regulation of the European Parliament and of the Council laying down harmonized rules for the fair access to and use of data: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

[18] Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0206

[19] Directive of the European Parliament and of the Council adapting the rules on non-contractual liability to artificial intelligence: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52022PC0496

Cybersecurity and cyber-resilience

Cybersecurity and cyber-resilience are the subject of several texts – and some others are coming.

- The Directive on the security of networks and information systems (the "NIS 2 Directive"), adopted on June 27, 2021, builds on the achievements of the NIS 1 Directive. Its objectives are to strengthen the security level of subcontractors in contact with critical IT infrastructures, to include local and regional authorities within the scope of the directive, and to broaden the sectors concerned from 19 to 35 (including waste management, postal services and agri-food).
- The Cyber Resilience Act[20], drawn up on the basis of the EU's 2020 cybersecurity strategy[21], also introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software. The aim of this text is to protect consumers and businesses from cybersecurity risks in their use of wired and connected hardware, as well as software.
- Finally, on January 16, 2023, the Digital Operational Resilience Act (known as the "DORA Regulation")[22] came into force, following its adoption by the Council of the European Union in November 2022. This innovative regulatory framework addresses the risks posed by the profound digital transformation of financial services, the growing interconnection of networks and critical infrastructures, and the increasing number and sophistication of cyber-attacks on financial sector players. The DORA Regulation provides, in a single legislative act and for the first time in the history of the European Union, a detailed and comprehensive framework on digital operational resilience for financial entities – for the time being. It also establishes a mechanism for the direct supervision of IT service providers at EU level.

[20] Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products incorporating digital elements and amending Regulation (EU) 2019/1020:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

[21] European Commission, "The cybersecurity strategy":
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[22] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector:
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R2554

Legislative cohesion: the great unthought of European digital policy

Following this period of legislative proliferation, European Commissioner Thierry Breton resigned and was replaced. In a report entitled *The future of European competitiveness*, the former President of the European Central Bank, Mario Draghi, identifies Europe's heavy regulatory burden as an obstacle to the scaling-up of tech start-ups[23].

The European Union seems to struggle applying its own rules, both to itself and to non-European players. It is therefore necessary to assess the regulatory landscape in which the European Union has chosen to live its digital future.

First of all, let's remind that the promulgation of these texts came at a time when the European Union was at an electoral and geopolitical crossroads, engaged in existential debates on various subjects such as the reform of the Common Agricultural Policy, health dependencies, energy, hosting and computing infrastructures, exacerbated by climate upheavals and geopolitical tensions heightened by the war in Ukraine and the conflagration in the Middle East.

What's more, the European Union is multiplying regulatory obligations that are likely to lead to numerous conflicts of competence between regulators – old and/or new –, since several of them will inevitably be charged with the same legislative objective, or with divergent objectives requiring arbitration. All without arbitrators or arbitration procedures.

By way of example, the issue of 'profiling activities' is not addressed in the same way in the GDPR as it is in the AI Act, which the European Union prides itself on the speed with which it is being drawn up. Yet AI regulation is agitating most of the world's states and, in each state, numerous existing or future regulators to regulate it. In 2024, the multiple layers of rules and competences linked to the design or use of AI is already creating a millefeuille of standards and regulatory competences, whose simple inventory is tedious and prioritization hypothetical.

When the biggest AI players forgo deploying their services in certain regions where the legal insecurity seems too high, their retreat in the face of the European regulatory challenge should make us wonder. If Europe scares them, should we be happy about it,

[23] Mario Draghi, "The future of European competitiveness. Part A: A competitiveness strategy for Europe", September 2024:
https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

or worried for our own European companies? What does this mean about the weight of this regulatory insecurity for a company of European origin?

In another sector, when a company is both an operator of vital importance and a bank or insurer, the question arises as to whether it should apply the DORA Regulation or the NIS 2 Directive, and whether it should see itself as a regulated financial organization or an IT service provider. Such basic and structuring questions were not envisaged by the European legislator. They emerged once the texts were juxtaposed and subjected to analysis by regulators from different backgrounds: in this case, cybersecurity and financial regulations.

The regulators responsible for consumer protection, freedom of communication and the protection of minors are different, making it difficult, if not impossible, to clarify their prerogatives when it comes to determining the extent to which they should rely on the DSA, the DMA, the GDPR, consumer law or competition law, to exercise their levers of action. The media and audiovisual sector, for its part, is wondering about the articulation between the DSA and the Audiovisual Media Services Directive (AVMSD).

On cybersecurity, the DORA regulation gives a place to financial regulators, taking them far from their core business. Unfortunately, they do not have – and will never have – the same level of in-house expertise, as regulators or government agencies dedicated to core cybersecurity issues and standards, with whom they will necessarily have to work. For the time being, the modalities of their cooperation are unclear, and it will be difficult for the issue to be settled by a court – be it judicial or regulatory –, whose role it is not to manage technical cooperation between independent administrative authorities.

With such exacerbated complexity, there is a risk that regulatory and legal disputes will precede the clarity of the rule and the predictability of its regulation.

To avoid such an outcome, it is more essential than ever to make up for the incomplete work of the previous European legislature: once an obligation has been laid down, who enforces it, with what consistency, what arbitration in the event of conflicts of jurisdiction and competencies, and at what speed?

The search for solutions to harmonize and rationalize the European digital legislative puzzle is urgent. It is essential to ensure consistent and effective application of the rules, and to avoid conflicts between the competent authorities. This is a task for political institutions, not for courts, and even less for arrangements between regulators.

In essence, by dint of filling so-called pockets of "lawlessness", European digital law contains zones of "over-rules" or "multiple rules". This is not due to a failure to designate regulators, but to the fact that they are superimposed beside each other, with no cross-cutting coherence mechanism.

All these regulators will be legitimate. They will all be attached to their turf. None will cede an inch of prerogative to another, unless forced to do so. But none is forced to. None has the mission of having a global vision of an activity, of a base of compatible obligations and of societal efficiency to guarantee compliance with all the rules – all legitimate – that are being piled up.

Judicial power: an answer to the lack of regulatory cohesion?

This wave of legislative adoption coincided with the first years of GDPR implementation, which benefited from two main sources of clarification: the European Data Protection Committee (EDPS), established by the GDPR, and the Court of Justice of the European Union (CJEU), including in areas not foreseen by the legislator.

For example, in 2016, the adoption of two texts – the GDPR and the "Police-Justice" Directive[24] - on the same day, seemed to distinguish between (i) public security and justice issues on the one hand, and (ii) privacy in commercial and private activities on the other. However, the CJEU decided to apply the European Charter of Human Rights to articulate national security issues with the principles of the GDPR, even though the European Union had never before defined or adopted a notion of "national security", since no member state is entitled to cede this area of its sovereignty to any European institution.

Thus, it becomes clear that administrative and judicial powers, delegated to independent authorities and judges over which the executive powers and national or European parliaments have no control, will be responsible for articulating these texts. However, regulators and courts have neither the prerogative, nor the culture, nor the institutional mandate to do so. What's more, in every EU Member state, the separation of powers manifests itself in a genuine articulation between them. When the legislature shrinks, the executive can increase its sphere of competence, which can lead to arbitration, often of a constitutional nature.

Under EU treaties and laws, what is known as the "principle of subsidiarity" represents a stratification of the respective competences of the EU and the Member States, but does not guarantee their articulation. When the European legislator adopts rights or principles that confer prerogatives on European litigants, institute sanctions and leave it up to the Member States to designate competent regulators, the lack of articulation between the

[24] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L0680

national and European levels mechanically blurs the chain of interpretation and encourages recourse to the courts.

However, no judicial remedy before the CJEU would allow the same litigant to challenge, in a single instance, divergent decisions issued by several regulators responsible for applying different texts in different litigious matters. The judge's role is to examine whether or not each regulator has erred in its interpretation of the text for which it is responsible. It does not involve arbitrating between legislative layers on behalf of the legislator, or deciding on the appropriateness or priority of applying one text rather than another. This would be an exercise reserved for the Constitutional Courts of the Member States or, where the European Convention for the Protection of Human Rights and Fundamental Freedoms is concerned, the European Court of Human Rights (ECHR). Strategically, to avoid such an arbitration of antagonistic principles and interpretations, it suffices not to refer a case to the ECHR, or not to be entitled to do so.

When the opponents of a text fail to prevent it from being adopted by the European legislator, they can rely on European disinterest in the actual implementation of adopted texts. This disinterest often translates into a lack of ambition regarding their execution, on the grounds that the European institutions will defer to the (bad, variable, inconsistent) will of the Eu Member states.

This raises the legitimate question of whether we are witnessing a shift from the separation of powers to the isolation of powers. When EU Member states themselves delegate (regulatory) enforcement powers to independent regulators, they are relying on administrations which, while independent, have no power to articulate their respective competences. Federal democracy has taught us that laws without federal powers generate jurisdictional conflicts and regulatory inefficiency. *Ultimately,* then, we may well ask whether the isolation of powers does not lead to the ineffectiveness of the law itself.

Do we need to legislate so much when we don't consider the risk of cumulating sometimes contradictory injunctions? This is a legitimate question when, having failed to provide the means to enforce laws, we can only consider sanctioning their non-compliance. The European Union sometimes deludes itself about the size of the sanctions handed down by its judicial authorities, whereas:

- sanctions for breaches of the law do not restore any competitive or economic balance: they do not resuscitate companies that have died of competitive injustice or legislative overload. They simply acknowledge the failure to enforce the law;

- exemplary sanctions do not impose a rule on players capable of circumventing or surviving it. They scare off the – European – competitors of the dominant players, unable to access the sophistication of the law and the complexity of its articulation in strategic decision-making and risk-taking.

What are the priorities for the new European term?

In order to overcome this situation, it is imperative that the new European term of office works to put in place procedural and interpretative texts to ensure effective articulation between major European legislative texts.

In the famous words of Jean-Claude Junker, *"We all know what to do, but we don't know how to get re-elected once we've done it"*.

Admittedly, writing procedures is tedious and has never got anyone elected or re-elected. But that's what makes a law, and therefore a political will, effective or ineffective. This regulatory streamlining measure, while likely to give the impression of slowing down processes, is in fact aimed at ensuring the transverse effectiveness of European digital law.

With this in mind, and in line with the EDPS guidelines of March 14, 2022 on the application of Article 60 of the GDPR on *"cooperation between the lead supervisory authority and other supervisory authorities concerned"*[25] , the EDPS has already affirmed its willingness to strengthen cross-border cooperation between the data protection authorities of the EU Member States, in order to ensure the effective and consistent application of the GDPR[26].

Similarly, it seems crucial to create mechanisms to coordinate the various pieces of legislation, especially those that are, rightly or wrongly, often coupled such as the DMA/DSA, the NIS 2 Directive/DORA Regulation, or the GDPR/Artificial Intelligence Regulation/Data Act and Data Governance Act. Such regulatory grouping is not conceivable without taking into account national levels: the relevant regulators may be new or existing, but their collaboration has sometimes not been foreseen by the European legislator.

In addition, it is becoming urgent to carry out impact analyses for all the texts mentioned, which are not just implementation analyses targeting each text individually. Of course,

[25] EDPS, Guidelines 02/2022 on the application of Article 60 of the GDPR: https://www.edpb.europa.eu/system/files/2022-10/guidelines_202202_on_the_application_of_article_60_gdpr_fr.pdf

[26] EDPS, Proposals for a better harmonized application of the GDPR: https://www.edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf

the latter should enable us to ascertain whether the legislation in question has borne fruit. But they should also make it possible to question their potential negative effects, their relevance *a posteriori*, any shortcomings, the cost of compliance for the various players involved, or potential contradictions with other texts.

Last but not least, it is essential to act quickly, because conflicting jurisdictions and challenges of articulation generate not only inefficiency, but also, and perhaps above all, long-term injustice and insecurity. In other words, when several laudable objectives are juxtaposed without regard for their articulation, all the hoped-for protections and guarantees may produce the opposite effects, and at the very least, none at all.

Author

Etienne DROUARD
Partner, Hogan Lovells (Paris)

Contributors

Jessica GALISSAIRE
Studies and Partnerships Manager, Renaissance Numérique

Anissa KEMICHE
European Affairs Delegate, Numeum

Samuel LE GOFF
Chairman, Renaissance Numérique

Jean-Luc SAURON
Senior civil servant and Professor, Université Paris Dauphine - PSL

Rayna STAMBOLIYSKA
President, RS Strategy

Director of publication

Jean-François LUCAS
General Manager, Renaissance Numérique

About us

Founded in 2007, Renaissance Numérique is an independent think tank dedicated to the digital transformation of society. It works to shed light on the changes that this transformation is bringing about and to give everyone the keys to mastering it.

Renaissance Numérique is a forum for debate and positive confrontation of expertise and ideas. It brings together academics, public figures, non-governmental organisations and businesses. Its reflections, widely disseminated via contributions, publications and events, are brought to the attention of public and private players at French, European and international level.

Renaissance Numérique is a member of the Observatory on Online Hate run by the French Audiovisual and Digital Communication Regulatory Authority (Arcom) and of the organising committee of the Internet Governance Forum (IGF) France.

Renaissance Numérique

Koburo, 35 rue Chanzy – 75011 Paris
www.renaissancenumerique.org

November 2024