AI IS LAW

Law, shield and spear of a European AI

Simon Bernard
Under the coordination of Arno Pons and Olivier Dion.

THINK-DO-TANK
DIGITAL NEW DEAL

May 2025

STATEMENT OF INTENT

This report is aimed at European, national and local public decision-makers, regulatory authorities and jurisdictions, start-ups and larger companies.

Public decision-makers. The report offers an overview of the rules that can be applied to stakeholders in order to better understand both their strengths and the challenges that companies responsible for implementing them may face. For legislators and governments, the report makes recommendations regarding the articulation, simplification, and standardization of certain rules. For all public decision-makers, the report offers a framework for interpreting how a legal framework can serve as a competitive advantage, including the need for virtue and respect for the rules to promote access to public procurement.

Regulatory authorities and courts. The report highlights two conditions specific to these institutions for the rule to be useful: (i) its application must be rigorous and uncompromising when the breach is proven and intentional, but (ii) its application must always be intelligible with the standards, to guarantee a favorable and predictable environment for innovators.

Startups and businesses of all sizes, whether they design or use AI. The first two parts of the report are designed as an educational tool, highlighting the strengths and areas of focus that legal tools can represent for the development of European AI. In its final part, the report can be seen by businesses of all sizes as a manual for the offensive use of the law, to turn perceived constraints into tomorrow's opportunities.

SUMMARY

"CODE IS LAW"
WAS A WARNING.
"AI IS LAW"
MUST BE A
WAKE-UP CALL.

PREFACE

In 1999, Lawrence Lessig formulated **"Code is Law"** in a book founder, popularizing the idea that computer code acted as law in the absence of explicit rules. A pioneering vision that became dogma, **this idea was quickly distorted by a libertarian movement that celebrates the primacy of code over democratic rules**, in the name of total freedom supposedly encouraging innovation. But this unregulated "freedom" has often resulted in abandoning democratic principles and leaving society solely to the interests of the large private players who control technologies.

Lawrence Lessig's message is not that "code replaces law," but rather that "code is a form of law—so it must be democratized." He warns against a shift in power: from law to code. This warning is more relevant than ever with the rise of artificial intelligence. Hence **the urgency of repoliticizing digital technology, so as not to leave it in the hands of libertarians who claim that "code is the only law that matters."**

"We must understand that code is never just technical. It is political."
Lawrence Lessig

Today, Simon Bernard updates this debate by asserting "AI is Law": he shows that artificial intelligence, like code yesterday, tends to become a new form of automatic regulation of behavior, raising new questions of control, transparency, and accountability. The author thus proposes an alternative to the illusion of a "free AI," recalling that, as with the early "free internet," the notion of freedom can be ambiguous: whereas Europeans understood "freedom" as a space of collective rights and guarantees, libertarians saw it above all as a liberation from legal and state constraints—in other words, an emancipation from the law itself.

This battle is undoubtedly the most decisive: that of Justice, that is, what is fair for all, and not for the majority, or worse, the most innovative. **Law is perhaps, at its core, the true common language of Europe.** This is why the legal question is central to the fight for digital sovereignty: to neglect it is to weaken the entire European project. "AI is law" offers a vision in which technology serves people, not the other way around. It is a way to ensure that economic development benefits the greatest number of people, while remaining faithful to Europe's democratic heritage.

« AI is law » is not a call for legalism or excessive bureaucratization. It is about bringing the law into line with technology, programming it as much as possible in software and systems, while ensuring the flexibility necessary for innovation. Successful integration will allow Europe to **defend its interests**, preserve its

culture, and **foster innovation**

To address these major challenges, this report puts forward proposals that are equal to the stakes. One of them alone represents the ambition: **to recognize code as the 25th official language of the European Union**. Such recognition would have a dual impact: on the one hand, it would protect the place of law in the face of the techno-messianic excesses of libertarians; on the other, it would require every European text to be able to be translated into executable language, **making law a lever for scalability thanks to its automatic applicability**. Probably the best possible operational response to the eternal question that the Digital New Deal has been facing since its creation: “regulation VS innovation.”

Arno Pons,
Digital New Deal

FOREWORD

"In recent years, we have developed increasingly complex systems to manage content on our platforms, partly in response to social and political pressure to moderate content. This approach has gone too far. We will now change this approach. We will end the current third-party fact-checking program in the United States and begin transitioning to a community ratings program."

In a press release dated January 7, 2025, the Meta group announced a radical change in the moderation of content published on Facebook, Instagram, and Threads, the group's social networks. Based on the model proposed by X, moderation will now be done with user ratings. This major change, justified by the desire to restore greater freedom of expression.

This decision is not a huge surprise, given Donald Trump's return to power. What is more surprising is the limited scope of the new moderation policy within the United States.

And if there was any doubt, a few days later, at the request of the Brazilian authorities, Meta confirmed: *"the change in policy at this stage only concerns the United States"*.

A digital giant since the early 2000s, the United States wants to remain so and dominate even more in the era of artificial intelligence. Two days after taking the oath of office, the new President was clear: "We are going to enter the golden age of America." That day, Donald Trump announced the StarGate project to achieve this, the development of infrastructure dedicated to artificial intelligence for a total amount of $500 billion over four years.

He also announced that he would roll back a 2023 regulation passed by the Biden administration that aimed to limit AI's security and transparency risks by implementing a series of safeguards. Specifically, these rules required developers to conduct a battery of safety tests to ensure that the systems they implemented were safe, particularly in terms of algorithmic bias.

This regulation had the virtue of responsibility and ethics. Above all, for the newly elected President, it had the drawback of being a "dangerous brake on innovation " through "a leftist vision that hinders the economic potential of artificial intelligence".

Economic potential and issues of power, technological domination, and national security, as OpenAI writes very directly in a report by positioning published on March 13, 2025[1], without any desire to hide anything springs from the predatory American attitude.

The billions are bound to catch the eye and suddenly remind us how the American

[1] Smart middleware funded to the tune of €150million by the European Commission, developed by the Sovereign-X and InfrateX consortia (initiated by Digital New Deal Do Tank))

giants took the lead, aided by massive financial participation from the United States, in 1992 and the election of Bill Clinton[2].

But deregulation should concern us at least as much.

TWO CONCEPTIONS OF LAW AND ECONOMIC ENVIRONMENTS

First, on the role of law. In our Romano-Germanic tradition, law is a tool for organizing our society, which is committed to equality of conditions. It is a set of rules, previously codified and hierarchized, which precedes customs to some extent. In the Anglo-Saxon system, the law is more based on precedents established by judges, which evolve according to the reality of practices, and strives to preserve freedoms.

Next, on the supervision of new technologies. Our regulatory culture tends to favor a precautionary principle. Technology is initially analyzed through the risks it presents to fundamental freedoms and rights, in particular. In Anglo-Saxon logic, usage more often precedes the rule, which will then provide corrections in the event that risks subsequently arise.

The return of this dichotomy of approaches, confirmed at the AI Summit co-organized in February 2025 in France with India, is the major difference with the era of the internet's emergence. At that time, new technologies escaped almost all rules. The internet was a network, difficult to touch, based on a technology that regulators struggled to understand. This further led to the idea that internet-related technologies could not be regulated.

In an article published in 1999, Lawrence Lessig, then a law professor at Stanford, prophesied, as a warning to our democracies, that with digital technology: ***« Code is Law." In other words, code - understood as machine language[3] - is intended to determine the rules of the game.***

* *
*

[2] From his first election in 1992, Bill Clinton passed a multi-year budget for civil research, a large part of which was allocated to high technology.

[3] This definition thus makes it possible to overcome the difficulty linked to the existence of different computer languages (Java, C++, Python, for example).

THE CODE IS POLITICAL.
AI WILL BE EVEN MORE SO.

INTRODUCTION

POLITICIZATION AND INCREASING REGULATION OF NEW TECHNOLOGIES

Twenty-five years later, it is clear that the subject has evolved considerably, and the opacity of the code can be more easily overcome in many areas. In Europe and throughout the world, a multitude of rules have emerged to bring order to the practices of certain players, more concerned with benefiting from the lucrative potential of the technology than its potential for general interest.

The share of the digital economy, which represents more than 15% of global GDP[4] and its impact on everyday life have led legislators to examine what could happen there and to seek to add rules to protect users.

Therefore, to encourage its massive development, it becomes necessary to provide some safeguards, without which only the interests of a few would be defended. The rule is a tool of trust.

In the European Union, since 2000, the directive on electronic commerce[5] laid the foundations for initial regulation.

In France, its transposition is carried out by the law for confidence in the digital economy (LCEN). Its explanatory statement is extremely clear concerning the ambition: "The adaptation of our law to the requirements of the development of the digital economy is necessary to strengthen confidence in the use of new technologies and to support the growth of this sector which, through its transversality, will be one of the drivers of economic dynamism in the coming years ".[6]

The texts have since evolved over time in line with technological discoveries, at the same time as the standard has been consolidated at the European Union level for the sake of efficiency.

Because digital technology, initially so difficult to grasp through a rule of law, has subsequently become so for a single State, the difficulty of **classifying virtual activities under a real rule becoming the difficulty of connecting virtual activities to a real State.** The European Union has become part of the solution. With its 27 countries, 23 million businesses, and nearly 450 million inhabitants, it is becoming difficult for a company, however powerful, to remove any connection to it.

The European Commission interpreted it exactly in this way when it laid the foundations for a digital single market in 2017. The economic aspects, with the abolition of roaming charges, and the technical aspects, with the cross-border portability of online content along with the prohibition of unjustified geo-blocking, had their legal counterpart with modern data protection rules, the now famous General Data

[4] World Bank report 2021. The report mentions that this share is expected to reach 20% of GDP in 2026..

[5] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce").

[6] Bill for confidence in the digital economy, tabled on January 15, 2003 by Prime Minister Jean-Pierre Raffarin and the Minister of Economy, Finance and Industry, Francis Mer.

Protection Regulation (GDPR).

Depuis, les pays de l'Union européenne se sont ensemble dotés de deux textes majeurs pour réguler les plateformes et les fournisseurs : le règlement sur les marchés numériques (DMA) et le règlement sur les services numériques (DSA). Et le 2 février 2025, un règlement sur l'intelligence artificielle est entré en vigueur. Comme pour marquer le changement d'échelle, ces textes sont d'application directe. En d'autres termes, leur entrée en vigueur n'attend pas une transposition de la part de chaque État[7].

Because economic initiatives have obviously not been lacking, but they are not enough. Regarding AI, President Emmanuel Macron announced, in a form of response to President Trump's StarGate plan, a massive investment plan in data centers. The law must therefore be an essential complement.

In this support for the law to impose our views and values on digital technology, the national legislature is obviously not left behind and is regularly attempting to accelerate and intensify regulation of the digital sector, sometimes with and often without the support of the Government. Thus, over the past 7 years, public order issues in the digital space have led parliamentarians to attempt substantial changes, which must now be understood as a clear politicization of digital issues. The law against hateful content on the internet of June 24, 2020, by MP Laetitia Avia, was a first shock, although largely censored by the Constitutional Council, before being amended as part of the law of August 24, 2021, strengthening respect for the principles of the Republic.

Three more recent laws should be even more striking, as they allow us to grasp the strength with which the national legislature is now interested in these issues, even if it means ignoring a European agreement.

First, the bills initiated by MPs Stéphane Vojetta and Arthur Delaporte to combat scams and the excesses of influencers on social networks, Laurent Marcangeli to establish a digital majority and combat online hate, and Bruno Studer to redefine parental authority and image rights. In both cases, the Government had raised objections because these initiatives preempted the work underway in Brussels. In both cases, these texts were adopted by a very large majority in Parliament, with minimal consideration given to the opinions expressed by the executive.

Then, the amendments proposed by Paul Midy and the Renaissance deputies, as part of the review of the law aimed at securing and regulating the digital space promulgated on May 21, 2024. This example is particularly strong in the sense that the deputies were trying to touch this time on the very identification of users.

Paul Midy, one of the rapporteurs of the text, proposed the implementation by 2030 of a certification procedure so that each connection to a social network could be subject to the presentation of a code.

A sort of license plate for the user of a social network. These amendments were ultimately withdrawn in light of the criticism they provoked and the risk they posed to the vote on the entire text.

[7] It is up to the States to adapt their internal law to give European rules their full effectiveness.

.

These initiatives therefore come up against differences in approach with European Union law, and the balance required by the Constitutional Council between the protection of privacy and freedom of expression.

Above all, they demonstrate the need for our companies to adopt a political interpretation of their models, that is, both the rules in place and the acceptable limits of activities developed in gray areas. Failing this, the legislator can now take up a subject at any time, without a trembling hand, even if it means flattening a model currently being developed. This is even more true in a political context that is now very unstable and in which the Government no longer benefits from a favorable balance of power with Parliament.

Also, monetizable digital object games have developed in recent years in a gray area. This is the case, for example, of digital cards representing team sports players, modeled on the albums of our childhood. Given the legal risk identified by gambling players, who also saw them as a formidable competitor, the legislature was asked to consider a proposal for an experimental framework. But following the debates, there was in reality little left of the flexibility previously enjoyed by the model, which is now largely constrained due to a failure to consider its acceptability by other stakeholders and its chances of prospering when it is brought before Parliament.

This is a major risk for many emerging activities, when 31% of French people say they are ready to trust AI, 69% doubt or are suspicious, 68% fear AI - making the French the most worried in the world, and 67% say that regulation is necessary[8]. In this same survey conducted by KPMG Australia and the University of Queensland on representative panels in 17 countries around the world, 96%

consider that the practices and principles of trustworthy AI determine the trust they place in AI systems.

In other words, the legislator, whether European or national, must be taken seriously and new activities constructed with a political interpretation, both for reasons of acceptability by the consumer and more broadly by the market, as well as by public decision-makers.

FROM THE CHALLENGE OF ACCEPTABILITY TO THE USE OF REGULATION FOR SUR- TO GO UP

This direct consequence of the growing and constant politicization of issues is not necessarily a constraint. If seized, it can be a source of great opportunity.

Because our law, often presented as restrictive, has become, over time, **an element of virtuous protectionism, confronted with actors without faith or law**, including now sometimes pushed by States to innovate without concern for standards.

[8] KPMG Australia and University of Queensland, "Do we trust artificial intelligence?" ", study published on February 6, 2024.

In this respect, the GDPR was initially seen as a false good idea, a rule that would prevent French and European companies from catching up with foreign giants in the data technology race. This, in theory, cannot be disputed, since some players are being forced to follow more restrictive rules to develop their business, after others have been able to do so freely..

A parallel could be drawn with the difficulty that emerging countries had to face when industrial countries decided to regulate global production and international trade, after having been able to develop with far fewer constraints.

But there is a major difference. In the case of the GDPR and other texts that the European Union is so vigorously imposing on itself, it is its values that it seeks to enforce. In other words, **the rules have a fundamental virtue: acceptability**. Would the growth of digital activities have been the same on the European market if it had not been regulated by rules on data protection and respect for privacy?

In this regard, it is worth noting that in 2018, in the midst of the Cambridge Analytica scandal - the massive exploitation of data from tens of millions of users on behalf of a company supposedly influencing voters' votes - Facebook announced that it was relying on the GDPR to "offer new privacy protection experiences to all its users." Two of the company's vice-presidents, quickly joined by Mark Zuckerberg himself, specified that these changes would apply worldwide[9].

These rules have a double advantage:

- They are a **protective barrier to the market**, both for the consumer, who then has products adapted to their values, and for companies, who cannot see competitors arriving on their playing field who do not respect their rules.
- In the event that foreign companies are subject to these rules in order to access the market, the European Union and its Member States are imposing a form **of extraterritoriality of their values through the standard**, by imposing demanding rules on any company wishing to benefit from the Union market.

The same extraterritoriality that the United States uses to weaken a competitor internationally through its anti-corruption rules or that China artificially creates within the framework of the Silk Roads, by making certain States captive by installing infrastructures at a cost disconnected from their capacities, before appropriating them for a long period thanks to the inability of the host country to appropriate them.

In this respect, the current legal framework seems less to constrain our companies than to allow them to **ultimately benefit from a competitive advantage in their domestic market, and to protect this market from the dire fate of a captive market of foreign interests so far removed from European humanist values.**

Because acceptability is a prerequisite for acceptance and then appropriation, which largely depend on the risks encountered by an activity and the behaviors adopted to respond to them.

[9] Meta press release dated April 17, 2018, "Complying with new privacy laws and offering new privacy protections to everyone, no matter where you live".

AI FACES THE MYTH OF PROMETHEUS

Artificial intelligence, as a "*tool used by a machine to reproduce human-like behaviors, such as reasoning, planning, and creativity*[10]," presents three main risks[11]:

• Individual risks.

Using personal data to train AI systems poses privacy risks, with data sometimes collected in a non-transparent manner or used for commercial purposes. This may be the case when collecting data when creating personalized content, such as a resume or medical analysis.

The risk of sensitive data leaks is also very high. Two main cases must be considered: that of an **AI that would use user data to feed learning algorithms**, and that of data collected without all the usual precautions. The first case is particularly evident in the context of conversational robots. Thus, the first versions of ChatGPT used for training the data that users entered for their commands to the robot. In this sense, ChatGPT received its first alert in March 2023, followed by a fine of 15 million euros, on the other side of the Alps, on December 20, 2024. The Italian data protection authority (Autorita Garante per la protezione dei dati personali), equivalent to the National Commission for Information Technology and Civil Liberties (CNIL), thus blocked access to the AI, considering that "*questions have arisen about ChatGPT's compliance with the European data protection regulation*." Access was finally granted a month later provided that the American company "*continues its efforts to apply European data protection legislation*."

The second case is not new and is related to ***scraping***, **that is, the collection of online data, protected or not**. The need to widely feed certain models has contributed to the expansion of this practice. However, even when data is publicly accessible, it cannot be used without all the usual precautions[12].

Besides these two topics, biases and errors can also be numerous.

Two patterns can then be represented: that of "involuntary" bias and that of deception. The first arises from a philosophical question, and leads us to wonder if bias is not ultimately the property of all intelligence, whether artificial or human?

The question that arises is to know which biases are acceptable. The second pattern can come from an error about the origin of content or even from deception initiated by the AI itself. Also, the AI Cicero developed by Meta to confront us in the geopolitical game Diplomacy quickly understood that it had an interest in lying in order to betray, contrary to the instructions given to it by its programmers[13].

From these issues emerges a fundamental question: who is responsible for an error made when using AI? What happens if an AI that promised to detect a serious

[10] Definition of the European Parliament. The elements of this definition distinguish AI from simple code or algorithm.

[11] In a report submitted on February 14, 2024, by MPs Philippe Pradal and Stéphane Rambaud, two risks were identified: individual risks and collective risks. It is appropriate to create an additional category with public order risks, given their importance and specific characteristics. Regarding the report: Report submitted in conclusion of the fact-finding mission of the Law Commission of the National Assembly on "the challenges of generative artificial intelligence in terms of the protection of personal data and the use of generated content."

[12] See in particular Articles 6.1.a and 21 of the GDPR, respectively on consent and the right to object; see also the work of the W3C for the creation of a technical standard for legal scraping https://www.w3.org/

[13] Manon Meyer-Hilfiger, "When AI Deliberately Lies to Us," November 30, 2024, National Geographic.

illness invisible to the naked eye misses it?

The success of the current transition to AI[14] agents therefore requires clear anticipation of this question of responsibility to avoid putting the models that will be developed at risk.

- **Collective risks.** Three major risks can be identified: cultural, so- social and environmental.

On a cultural level, generative AI presents several risks. First, **in terms of information, with the development *of deepfakes***, combined with the increased visibility of social networks. Second, there is a risk of standardization of content and less reward for original content, which is necessarily more expensive to produce. The film industry is an example of this, with the long-term writers' strike in Hollywood in 2023 or the recent shocks suffered by voice actors given the possibility of replacing human doubles with artificial ones, with a tone of voice identical to that of the original actor.

On a societal level, AI presents both a risk in terms of discrimination, since an algorithm could amplify a gender or origin bias that would be present in the training data, and a risk in terms of the protection of human rights. This second point is little noted but is nevertheless very real: significant human resources are required for learning and proper functioning of artificial intelligence, with their particular responsibility of annotating data. However, these human resources are often located in countries once considered the world's workshops. India is a striking example, with more than 70,000 people employed for this purpose by the end of 2024[15].

On the environmental front, a recent report by the Capgemini research institute reveals that training a model the size of GPT-4 consumes the energy needed to power 5,000 American homes for a year. The same report reveals that water consumption by the Data Center Alley technology infrastructure installed in Virginia increased by 69% in 2023 compared to 2019 levels. However, according to this study, only 12% of companies measure the environmental impact of generative AI and 74% acknowledge a lack of transparency in environmental measures on the part of generative AI solution providers. This, while the carbon footprint of digital technology already represented at least 2.5% of the French carbon footprint in 2023[16].

Added to this is the construction of infrastructure in spaces where it can endanger the local environment. A Google data center project 30 kilometers from Montevideo, the capital of Uruguay, caused controversy in 2024. The project, which had obtained environmental permits, required the daily consumption of up to 55,000 Uruguayans, while the country was experiencing a major water crisis. To overcome this difficulty and allow the project to go ahead, the company subsequently revised its plan and ensured that the cooling technology would use air.

Societal and environmental risk is one of the major challenges of AI: extractions

[14] AI agents can be defined as systems designed to perceive, interact, and make decisions. independently.

[15] Clément Perruche, "In India, the little hands that feed AI models», October 27, 2024, Les Échos..

[16] Figure given by ADEME and Arcep in 2023. According to The Shift Project, the carbon footprint of digital technology would increase by 6%/year on average.

of rare minerals capable of boosting the technology are numerous, the activity of the systems and the conservation of data consume enormous energy, and the hidden side of the learning of these systems reveals significant human resources made up of often low-cost labor to ensure that the technology learns properly and does not stray into undesirable areas.

- **Public order risks.** While AI has made it possible to detect more risks, it has also increased the risk of disruptive activities and cyberattacks, by further exposing providers of new technologies given the data they are likely to manipulate.

First, AI allows certain practices that may be deemed contrary to European values, such as social rating systems that could threaten the general organization of a state or a system it organizes, and therefore public order. This would be the case, for example, of AI that would use data on a person's actions to rate them and thus determine their right to access social assistance or social housing.

Then, easy-to-use AI tools are used to perform large automated phishing attacks, identity theft or sophisticated schemes to deceive potential victims, and for the creation of malware to circumvent security rules.

Thus, in February 2024, the generation of a deepfake using AI allowed scammers to steal $26 million from a multinational corporation by posing as senior executives. The scam began as a classic one, with an email sent by someone claiming to be the London-based CFO. But the employee had some doubts. A video conference was then set up to reassure him. On the screen, the employee recognized the faces of his colleagues. The employee was reassured and complied, paying the requested amount. Except that the faces on the screen were all fake and generated by downloading all the videos of the company's employees available on the internet.

These new tools are also being used by state-affiliated groups to prepare their attacks. For example, OpenAI and Microsoft have identified five actors affiliated with China, Russia, North Korea, and Iran using AI tools to enhance their attacks[17].

These risks can be obstacles to innovation, as soon as the technology is not deemed acceptable by the user. This scenario is not new and has been clearly identified over time with regard to past innovations in other sectors: nuclear power required significant control rules after the Chernobyl tragedy and even today a change in the regulatory framework is causing widespread concerns[18], while mentalities are evolving but less than half of French people are in favor of it[19], and genetically modified organisms (GMOs) have for the most part not resisted drastic regulation or even a ban given the concerns they raised for health, the environment

[17] Blog post published by Microsoft Threat Intelligence on February 14, 2024, "Staying ahead of threat actors in the age of AI."

[18] In 2023, during Parliament's examination of the law aimed at simplifying procedures related to the construction of new nuclear reactors, the proposal to merge the regulatory authorities (Nuclear Safety Authority) and the Institute for Radiological Protection and Nuclear Safety (IRSN), for example, provoked a strong reaction from parliamentarians of all stripes. The merger was ultimately only possible in another law, after additional and in-depth impact studies.

[19] En 2023, lors de l'examen par le Parlement de la loi visant à simplifier les procédures liées à la construction de nouveaux réacteurs nucléaires, la proposition de fusion des autorités de contrôles (Autorité de sûreté nucléaire) et Institut de Radioprotection et de Sûreté nucléaire (IRSN) avait par exemple suscité une vive réaction de la part des parlementaires de tous bords. La fusion n'avait finalement été possible que dans une autre loi, après des études d'impact complémentaires et approfondies.

and biodiversity, despite the advantages they could represent.

To ensure the smooth and useful development of this technology for all, our companies, and those that decide to enter the European market, must therefore respect the rules of the game that limit these three risks as much as possible.

LAW IS CODE: FOR A VIRTUOUS, SUSTAINABLE AND COMPETITIVE AI

To create a framework favorable to the development of a technology, two approaches are possible: on the one hand, laissez-faire and self-regulation; on the

other hand, founding regulation, laying down clear rules from the outset in order to guarantee that this technology evolves in accordance with the major principles of our society.

Regarding AI, the Americans have chosen the first path. The Chinese are moving toward the second. The European Union has the conditions to take the second path before anyone else, but some are still reluctant to do so, at the risk of either being dominated by the Americans, for failing to master and take advantage of the second path, or by the Chinese, for failing to impose its rules. The European Union must therefore succeed in imposing this third digital path, the one that allows us to move from the rule of law to the rule of fact. A fully democratic right.

It is an undeniable fact that in Europe, the regulatory environment has become omnipresent and has taken on considerable weight.

The regulatory environment is made up of rules dedicated to digital technology and rules that are not intended for it but can have a very structuring scope.

These rules actually show a clear path for the development of AI European: ethical, safe and sustainable.

First, the rules dedicated to digital technology offer a clear line to defend-create ethical and safe AI.

Then, traditional rules of law draw lines of balance that can facilitate the creation of original AI between tradition and disruption. They are complemented by sustainability rules, which provide a horizon.

To achieve this ambition, however, the law must no longer be a mere translation of intentions, but must be transformed into a weapon serving French and European ambitions. An economic weapon, and above all, a strategic and global weapon.

It is therefore both the observation of growing and imposing regulation, and the strategic necessity of law in the service of innovation which dictate the approach of this report.

* *
*

With the arrival of generative AI, we are facing what the Digital New Deal calls: GenAI = Web². In other words, a phenomenon of increased centralization of power and massive capture of value, amplified by the multiplied capabilities of this new technology[20].

We must not repeat the mistakes of 25 years ago. Because at the risk of amplifying the current influence of a handful of giants, we now have an avowed libertarian vision, brought to power by the world's leading technology nation.

It is therefore imperative to arm ourselves politically, by making the law our first priority. This requires a new approach to regulating artificial intelligence, which by structuring this key sector, will mechanically shape the entire digital economy of tomorrow.

As the United States embarks on a mad race without rules, and China pursues it with great opacity and the desire to impose its own rules of the game in the future, France and the European Union must adopt a modern regulatory approach to maintain balance: limiting the risks that technology presents, while slowing innovation as little as possible. A constructive response to the limits of the law exposed by the Draghi report[21]. A response with a new, strategic, and global approach, closer to the proposal in the Letta report[22] for a 28th virtual state to standardize the rules governing the production, distribution, and sale of goods and services in the European Union. A proposal also taken up in Mario Draghi's report.

Our companies can adopt an AI governance strategy that maintains this precarious balance between innovation and protection of the public interest, limits risks and guarantees safer development.

It is up to politicians, then, to impose a new vision of law in the service of innovation and to channel their recent propensity to constantly regulate digital technology, and for regulators and jurisdictions to firmly apply the rules. Thus, Europe will take, through law, a serious step towards a destiny of excellence in terms of AI and AI practices.

[20] "Generative AI: unite or suffer" by Olivier Dion, Michel-Marie Maudet and Arno Pons, October 2024.

[21] Mario Draghi's report to the European Council, "The future of European competitiveness", September 2024.

[22] Report by Enrico Letta presented to the European Council, "Much more than a market", April 2024.

AI IS NOT THE LAW:
IT IS A POWER.
IT MUST BE MADE
DEMOCRATIC.

I.ETHICS AND SECURITY TO UNLEASH AND DEFEND INNOVATIVE POTENTIAL

The first rules that make up the legal framework for artificial intelligence are the most prominent: those relating to data, particularly the GDPR and the AI Act. Next come cyber standards.

A. DATA AND USAGE ETHICS AS A STANDARD MARKET ACCESS

These rules deserve serious discussion, as they are widely criticized and criticized as major obstacles to innovation. These rules do indeed pose barriers, but they are also often the subject of spurious lawsuits and can, on the contrary, be valuable allies for our businesses, provided that some complexities and difficulties of use are overcome .

Data and usage protection is first and foremost an aquarium in which a product bathes to ensure its smooth development. This protection is then what must force other daredevils, those without faith or law, to adopt virtuous rules in turn, or risk being excluded from the markets.

1. Supervision of data and uses to build on sound foundations

In 1950, Alan Turing published an article entitled "Computing Machinery and Intelligence," in which he discussed his intention to endow machines with a form of intelligence. During this period, a large number of ideas flourished, from a chess-playing machine to one that would automatically translate text into a foreign language.

In 1997, artificial intelligence came out in its evening gown when Deep Blue, a machine developed by IBM, beat Garry Kasparov, world chess champion, in a second match of six games.

However, it wasn't until the 2010s that artificial intelligence reached the heart of the city and became widespread. One of the main reasons: the maturity of computing and the internet created a gigantic amount of data that made it possible to easily and widely feed these machines.

The world of innovation has just discovered the existence of wells filled with hydrocarbons capable of multiplying the capacities of a machine.

This hydrocarbon that is data already serves digital engineering. Legislators at national and European levels have taken it up.

The GDPR is arguably the most well-known legal framework regarding data protection. It came into force in May 2018 and imposes strict obligations on companies regarding the collection, processing, and retention of personal data .

When it comes to artificial intelligence, the GDPR, given its age, is the first legal entry into this new world. On April 8, 2024, the CNIL published its first recommendations to provide companies with concrete answers to the legal and technical challenges related to the application of the GDPR to AI.[23]

On February 7, 2025, the CNIL published two new recommendations, also illustrated by numerous examples and concrete solutions. This time, they particularly concern information and the exercise of the rights of individuals whose data is used.

Non-personal data regulation, data act and data governance act. In addition to the GDPR, there are two regulations[24], less well-known to the general public, which came into force later. This time, the aim is to eliminate obstacles to the free flow of personal and non-personal data between different EU countries, within businesses and the public sector, and thus guarantee both their availability and security, as part of the **European Data Strategy**, presented in February 2020.

The *Data Act* and the *Data Governance Act* are offensive regulations on which Digital New Deal has worked extensively in recent years (three think-tank reports and three consortia dedicated to data sharing initiated by the do-tank). They allow for what Digital New Deal has been calling for since its creation, namely the possibility of benefiting from the Metcalfe effect[25] in order to be able to compete with American and Chinese groups that take full advantage of network effects[26].

It is this strategy that we often need to return to, because it carries the ambition to elevate European AI: to enable all public and private actors in the European Union to benefit from high-quality protected data.

Artificial Intelligence Regulation (AI Act). The existence of data of all kinds in very large quantities has therefore led to the development of AI for the general public, consisting of businesses and individuals.

Also, if the GDPR already made it possible to regulate this emerging market from the end. In the 2010s, it quickly became a question of looking at uses: automation of tasks, use of data to better predict or identify, assistance with decision-making, personalization of recommendations or content, autonomy of objects, writing or creation.

The emergence of a multitude of these uses in industry, health, agriculture, commerce, marketing, office automation, mobility, education, security, culture, and leisure have led legislators, and in particular the European legislator, to seriously consider the legal framework specific to artificial intelligence.

A reflex activated by the high risks for public interests (health, security, fundamental rights including democracy, the rule of law, environmental protection[27]) given the

[23] This first series of recommendations follows the launch by the CNIL in May 2023 of an "AI plan", in order to clarify the legal framework and provide greater security to stakeholders.

[24] Data Act and Data governance Act.

[25] This law states that the value of a network is proportional to the square of the number of its users. Like Moore's Law for computing power, Metcalfe's Law is a major theoretical foundation for understanding the growth dynamics of digital platforms and online services.

[26] Concrete example: Spotify is the only European big tech company thanks to Metcalfe's Law. It's not just an audio streaming platform, but a music social network (users are reluctant to leave Spotify for Apple Music to avoid losing their playlists, their friends, etc.)

[27] These risks are cited in point 8 of the recital of the AI Act.

announced power of the uses permitted by artificial intelligence.

Because, if in this context still there are criticisms concerning the constraints that rules impose, it is above all to allow the development of innovation that this was thought of.

If we were to allow AI to develop for scoring access to bank credit, at the same time as AI to better treat cancer using an individual's health data, would the latter survive the former?

2. The AI Act: the misunderstood who wanted to do good

In April 2021, the European Commission published the draft regulation "Artificial Intelligence Act", which would become the AI Act three years later. From that date, the proposal displayed a clear ambition: to prepare the European Union to become a world leader in artificial intelligence, driven in particular by France, which published its strategy to unite stakeholders (France IA) in January 2017 at the initiative of Axelle Lemaire, Secretary of State for Digital Affairs, and Thierry Mandon, Secretary of State for Higher Education and Research.

The recital of the AI Act is absolutely clear on this point: "*By establishing these rules, as well as measures to promote innovation with a particular focus on small and medium-sized enterprises (SMEs), including start-ups, this Regulation contributes to the achievement of the objective of promoting the European human-centric approach to AI and making the EU a global leader in the development of safe, trustworthy and ethical AI, as formulated by the European Council, and it ensures the protection of ethical principles expressly requested by the European Parliament*[28]."

This reminder of the objective is essential because it goes against the current of criticism that quickly emerged regarding the limits that the regulation would impose on innovation. In other words, many entrepreneurs have noted that France and Europe risk once again missing out on the AI revolution, after that of the Internet, because of its overly rigid frame.

However, going into the main principles of the text leads to the conclusion that it is in favour of a text that is consistent with its objective as initially set out, as the text seems to be going in the right direction and taking into account the major issue of acceptability, a sine qua non condition for the development of AI in Europe.

[28] Point 8 of the recital of the AI Act.

THE AI ACT: DEFINING RISKS, PROHIBITING THE UNACCEPTABLE AND SUPERVISE THE MOST SENSITIVE USES, ENSURE A MINIMAL TRANSPARENCY

The AI Act is coming into effect in stages. Its first part, which came into force on February 2, 2025, focuses on classifying AI by risk level and prohibiting those that pose unacceptable risks. This includes social rating systems, AI for mass surveillance or for assessing an individual's criminal risk based on biometric data, or AI designed to deliberately manipulate or deceive an individual.

The European Union has taken the initiative to propose a legislative framework to regulate the use of AI through the AI Act (proposal for a regulation on artificial intelligence), presented in April 2021. This regulation aims to establish a coherent approach to the regulation of AI in Europe, taking into account the risks associated with these technologies and emphasizing safety and ethics.

Banning the Unacceptable[29]. The regulation classifies AI systems according to their risk level, from "low risk" to "high risk," and imposes obligations based on this classification. For example, systems used for high-risk applications, such as AI applied to health or public safety, will have to meet strict requirements for transparency, conformity assessment, and ongoing monitoring.

This should be particularly the case for an application such as Clearview AI, already sanctioned by the CNIL and its Italian and Dutch counterparts for breaches of the GDPR. This company, established outside the European Union, offers a search engine for images of individuals, based on mass extractions from the internet, including of individuals established in the European Union. The app user can then submit a photo to verify the match with the person registered in the system, in the event of an arrest by the police, for example.

It is therefore very clear that the prohibited uses are strictly contrary to our values. And there would certainly be no circumstances that would allow them to be exploited on the European market, so divisive would they be. The distrust they would arouse would, on the contrary, reflect on all AI entrepreneurs.

Regulating high-risk systems[30]. The AI Act then defines high-risk systems. These are those that may jeopardize the security of individuals or their fundamental rights and thus justify subjecting their development to enhanced requirements. These requirements include conformity assessments and technical documentation of risk management mechanisms. The systems concerned are listed in two annexes to the regulation: products that are already subject to market surveillance in Annex I (which include medical devices, civil aviation security, or vehicles) and those in eight specific areas in Annex III (biometric systems, critical infrastructure, education, employment, access to essential public services, law enforcement, immigration, and the administration of justice).

Remain vigilant in the event of a specific risk. A third category is provided for AIs that present a specific risk, for example in the event of a clear risk of manipulation. This category remains broad since the use of a chatbots may be affected. In this case, transparency obligations are provided for, without any other constraints.

The fourth category of AI classified by risk level is that of minimal risk systems. In this case, no specific obligation is provided.

The special case of general-purpose AI. Beyond AI classified by risk level, the AI Act addresses a special case, which was not initially planned and was added during debates in the European Parliament: that of general-purpose AI.

That is, AIs that perform a large number of tasks and are therefore very difficult to classify into one of the four risk categories.

This is exactly the case with generative AI and in particular large language models (LLM) such as ChatGPT, DeepSeek or Le Chat de Mistral AI.

For these AIs, various obligations are provided. These obligations include minimum

[29] Article 5 de l'AI Act.

[30] Article 6 de l'AI Act.

transparency and documentation measures regarding the capabilities and limitations of the system, as well as regarding copyright and related rights, and the content used to train the model[31].

These minimum obligations may be supplemented by other obligations[32] when the model presents a systemic risk such as its use for cyberattacks or biases with discriminatory effects[33].

Seven criteria can be used to assess this impact[34] : the number of model parameters, the quality and size of the training data, the amount of computing used for learning, the model's input and output methods, the assessment of the model's capabilities, the model's impact on the domestic market, and the number of end users.

RISK LEVEL	OBLIGATION	EFFECTIVE DATE
Unacceptable	Prohibition	February 2, 2025
Hight risk	Reinforced requirements	August 2, 2026 for Annex III and August 2, 2027 for Annex I
Specific risks	Transparency obligations	August 2, 2026
Minimal	No specific obligation	
AI THAT CANNOT BE CLASSIFIED BY RISK LEVEL		
General purpose AI	Different levels of bonds depending on risk	August 2, 2025

Exceptions pour favoriser les innovations. Exceptions to promote innovation. And for those who persist in the idea that the AI Act would definitively "kill innovation," the latter also introduces "regulatory sandboxes"[35], controlled environments where AI systems can be developed, tested, and validated before being put on the market. These sandboxes make it possible to identify and mitigate risks related to fundamental rights, to health and safety. They also provide guidance on regulatory expectations and requirements. A successfully tested AI system in a sandbox can serve as proof of regulatory compliance, facilitating cross-border cooperation and the sharing of best practices.

Presented this way, the legal framework governing the use of AI, both for data and for its uses, appears to protect rather than constrain. It prohibits the unacceptable and regulates what is sensitive. Our legal framework thus creates a protective layer likely to facilitate the acceptability of new uses by a curious but fearful market.

[31] Article 53 of the AI Act.

[32] Article 53 of the AI Act.

[33] Article 53 of the AI Act.

[34] A presumption of high impact, therefore of systemic risk, is established by Article 51 of the AI Act for cases where the cumulative volume of calculation used for training the model is greater than 1025 floating point operations per second (FLOPS).

[35] Article 57 of the AI Act.

EXCEPTIONS TO PROMOTE SMEs

The AI Act contains a series of measures specifically designed for SMEs to support and simplify their compliance. Regulatory sandboxes will be accessible free of charge and as a priority to SMEs, with simple procedures. Scheme assessment fees will be proportional to the size of the SMEs, and the issue will be regularly assessed by the Commission, with adjustments made as needed. The Commission will develop simplified technical documentation forms, along with dedicated training. Specially designated channels will also be created to facilitate compliance for SMEs. Finally, the obligations imposed on general-purpose AI providers are appropriate and proportionate. Thus, the code of practice must include specific performance indicators for SMEs.

THE PRECEDENT OF THE BAD TRIAL OF THE GDPR

Even before the AI Act, the GDPR had been accused of blocking innovation.

Because it forces the classification of data that is sometimes difficult to contextualize and increases transparency obligations, the texts on non-personal data add further obligations regarding data that do not, however, endanger anyone's freedom or privacy.

These frameworks also create significant litigation risks that could pose a challenge to any company that tries to avoid them. The fine can be as high as 4% of annual global revenue, and the publicity that can result adds to the negative consequences.

In 2021, Amazon Europe Core was fined €746million at first instance[36] for non-compliance with the GDPR by the French National Commission for Data Protection (CNPD), the local equivalent of the CNIL. The regulator accused it of failing to comply with the European framework, particularly in the collection of its users' data. Amazon had already been fined by the CNIL in 2020 for non- compliance with the rules concerning advertising trackers (cookies).

This sanction illustrates the consequences that non-compliance with the GDPR can have, and remains unprecedented in its scale. Google, for example, was sentenced to two fines by the CNIL, also for non-compliance with the rules on advertising trackers due to failure to comply with the obligations regarding the collection of user consent, but this was capped at a cumulative amount of 100 million euros[37].

Beyond the fine, the simple formal notice can put a company that does not have the financial backing of a giant.

On February 5, 2020, Olivier Magnan-Saurin, co-founder of the startup Fidzup, posted an article titled "The CNIL killed me"[38]. This company had been marketing geolocated marketing campaigns to attract consumers to a physical point of sale (a "drive-to-store" model) for nearly nine years and had been placed in receivership two months earlier. The reason given? A formal notice made public by the CNIL in July 2018, at the same time as two other startups in the sector, which had managed to relaunch after compliance[39]. The entrepreneur then explains that this publicity

[36] An appeal procedure is underway. The company accuses the regulator in particular of not having allowed it to modify its practices, before imposing such a fine on it.

[37] These two fines were confirmed by the Council of State on January 28, 2022. Decision No. 449209 of the 10th and 9th Chambers reunited.

[38] Article posted on Medium, February 5, 2020.

[39] Teemo (since acquired by the Near group), Vectaury (since acquired by Mobsuccess) and Singlespot.

made it almost impossible to develop the application, in the midst of the market's evangelization.

The CNIL then deemed it necessary to "alert the millions of people whose data was being collected and processed without their knowledge." This public notice also aimed to prevent the development of this model "based on such practices" by sending a "collective alert."

If the start-up Fidzup did not manage to overcome the formal notice, Singlespot, Another of the start-ups involved has made it a marketing asset.

While facing significant questions about the legal framework and a major challenge in terms of market acceptability of the offer, the startup turned the formal notice in its favor. Thus, Thomas Opoczynski, co-founder of Singlespot, explained that the implementation of the GDPR had held back some customers, given the risk they incurred if they worked with a startup whose compliance with the legal framework was not certain.[40] The procedure opened with the CNIL allowed them to open a new commercial field, by clarifying this point.

As early as 2018, the CNIL dared to say: "If you comply with the GDPR, you will have a competitive advantage!"[41]. A 2022 study, carried out by the CNIL's digital innovation laboratory (LINC) and a literature review published on March 1, 2024 by the European Review of Media and Digital Technology tend to confirm this approach, with balance and nuance, although advantages and disadvantages can be noted in both directions and a greater advantage seems to emerge for larger companies.

3. Where the shoe can really pinch: better articulate the rules between them

Our contemporary protections are not in themselves a nuisance, and the opposite has been proven. What can render certain data unusable or prevent potentially useful practices is in fact the proliferation of rules, particularly sectoral and liability rules, which adds to the complexity without the added value becoming evident. However, it is at this point that doubts about the usefulness of a rule can arise.

A complementarity between the AI Act and the GDPR needs to be clarified. At first glance, the AI Act is highly complementary to data-related legislation, including the GDPR. One is concerned with data, the other with artificial intelligence systems. The GDPR, for example, applies simultaneously with the AI Act whenever personal data is involved.

However, several difficulties must already be addressed.

Regarding the supervisory authority[42], on the one hand. The CNIL is obviously responsible for matters relating to the GDPR. This is much less obvious regarding the AI Act, which is more of a product regulation and would therefore encroach on the turf of dedicated sectoral authorities.

The training and expertise of the General Directorate for Competition, Consumer

[40] Géraldine Russell, "How Singlespot dealt with the CNIL's formal notice," Maddyness.com, November 29, 2018.

[41] CNIL, Practical guide to raising awareness of the GDPR, 2018.

[42] Article 70 of the AI Act.

Affairs and Fraud Control (DGCCRF) can in this sense be seen as an asset, if it is a question of only arresting a single reference authority.

But an alternative could be found in the model chosen by Ireland, which has designated sectoral regulators as competent national authorities[43]. This should enable companies and public entities to ensure that exchanges take place at a high level of technical and sectoral knowledge and thus facilitate the implementation of new requirements, provided that good coordination with the CNIL is ensured, without one overflowing into the competence of the other.

Assuming that the financial and human resources of each of the authorities selected are sufficient, this solution could be the most likely to respond to the challenges and balance between regulation and innovation. This could avoid adding sectoral friction because, on the other hand, the GDPR and the AI Act already have some clearly identified areas of friction.

This is the case of the conditions of anonymization and pseudonymization of data, considered too strict by many actors, preventing the use of certain data as training data.

The issue of data retention periods. This is also the case for data retention periods, which present the same pitfall. However, this issue is often misunderstood, including by the regulator. In recent years, two issues of general interest have come close to failing for this reason.

First, in the context of the covid crisis, when the government had proposed the establishment of consolidated files for research and epidemic control purposes. The aim was to allow data to be retained for a certain period of time so that information systems would have enough information to make it relevant. However, with each text on the health crisis, the subject came up again and parliamentarians discussed reducing the retention period.

Then, in the context of the experimentation of intelligent video for the maintenance of public order, in view of the Paris 2024 Olympic and Paralympic Games. Here again, it was a question of starting the experiment early enough to train the technology before the event, and stopping it late enough to consider keeping the technology afterwards, by moving forward with a sustainability law, otherwise, everything would be lost in the meantime. And this time again, the retention period was the subject of long exchanges and debates, many parliamentarians thinking it possible to have a technology and the data that goes with it only a few days during which it is useful. Ignoring all the training rules.

On this point, a balance will necessarily have to be sought again, making the best use of the flexibility provided by the GDPR for research purposes in particular[44], to ensure a fine balance between the protection of public freedoms and the competitiveness of our AI. This is particularly true in areas of general interest, very well covered and defended by the AI Act, notably thanks to regulatory sandboxes. Much less so by

[43] Eight sectoral authorities were selected: the Central Bank of Ireland, the Commission for Communications Regulation, the Commission for Railway Regulation, the Competition and Consumer Protection Commission, the Data Protection Commission, the Health and Safety Authority, the Health Products Regulatory Authority, and the Department for Transport's Marine Investigation Bureau.

[44] Article 5 of the GDPR, in particular e).

the GDPR when the two texts come to be articulated, while the sole principle of data minimization seems to be in contradiction with the needs of an AI, which is moreover generative. All the more so since at this stage, in the event of a conflict, it is the GDPR which prevails.

The CNIL's regularly updated practical recommendations and the recent December 2024 opinion of the European Data Protection Supervisor are important first steps to avoid areas of friction but are not sufficient to remove the stumbling blocks, particularly those presented in this way[45].

Conflicting interpretations between authorities within the European Union. Another complexity arises from the divergences in interpretation between national authorities within the European Union. The GDPR, in particular, although European, can be interpreted differently from one country to another, without harmonization being possible within even a reasonable timeframe, creating a major point of friction for the innovation and deployment of French and European AI, while other foreign AIs benefit from more flexible interpretations.

Thus, Ireland, which was recently able to toughen its position regarding IA[46], is regularly singled out for its lax reading of the GDPR while the principle of the single window makes it the lead authority for cases involving companies established on its territory, that is to say the majority of tech giants.

The Data Protection Commission, the equivalent of the CNIL for Ireland, thus requested in December 2022 the partial annulment of binding decisions issued by the European Data Protection Board (EDPB) in the context of the monitoring of the Meta group's networks and applications. The General Court of the European Union rejected the request in January 2025[47].

The fact remains that the cooperation mechanism provided for by the GDPR must function fully and objectively so that European texts do not become a burden for French and European companies, but rather a protection in their development.

The EDPB's (European Data Protection Board) 2024-2025 strategy, announced in April 2024, moves in this direction by including harmonization between Member States and effective cooperation between data protection authorities among its pillars. Concrete responses to these various points could be usefully provided within the framework of the omnibus announced on March 13, 2025, by European Commissioner McGrath. This next package should simplify the GDPR, particularly the compliance of very small businesses.

[45] Among other issues, a communication from the European Parliament dated February 2025 identifies a conflict between the AI Act and the GDPR regarding algorithmic discrimination. While the AI Act provides for the possibility of using specific personal data to avoid bias and discrimination in high-risk systems, the GDPR then too broadly restricts the legal bases making the use of this data possible. The GDPR therefore renders the provision of the AI Act inoperative.

[46] In 2024, the Irish CNIL reminded Meta and X of the exploitation of personal data by their LLM. An investigation has also been opened concerning Google.

[47] General Court of the EU, 29 January 2025, joined cases T-70/23, T-84/23 and T-111/23.

THE STANDARDIZATION OF THE RULE OF LAW AS LEGAL SECURITY

A first response to conflicts of interpretation could be provided by a more codable mechanism of the rule of law, whether it concerns hard law or soft law texts.

Because with AI and dedicated infrastructures, if data and uses multiply, so does automation. Thus, to take the example of data sharing spaces (data spaces)[48] supported by the European Commission to allow European actors to benefit from high-quality shared data, these data spaces maintain each actor in their role as data manager but create rules for circulation and processing between actors based on sectoral use cases.

These rules and use cases are provided for by a "Rulebook". However, if the law is clear and easy to translate into code, it will allow the "Rulebook" a standardized implementation of these sharing spaces.

However, while the AI Act is largely similar, other texts, including the GDPR, could still be improved to facilitate this. A dedicated omnibus could be considered as an extremely favorable signal for innovation in the coming months.

Liability regimes and legal uncertainty. In February, the European Union withdrew its draft directive on AI liability. This text aimed to harmonize the liability rules of the 27 countries in matters of AI, reduce the burden of proof for victims of damage caused by AI systems.

As a result, liability rules for AI will at this stage remain divided between the general liability regimes of the Member States and the special liability regime for defective products. It is, moreover, the existence of the latter regime that tends to rationalize the choice of pausing, perhaps definitively, a liability regime dedicated to AI. Because while the updated directive on liability for defective products[49] still needs to be transposed by the Member States, it usefully and broadly takes into account developments related to digital technology and in particular the uses of artificial intelligence.

This articulation is not in itself a heresy and presents a certain coherence. But it can create real legal uncertainty in the pitfalls of defective products, certain uses of AI and in certain cross-border cases that quickly arise.

It will therefore be necessary to ensure that these cases of uncertainty are quickly overcome and, above all, that they do not benefit the most powerful new technology companies which will tend to respond to the question of responsibility in their contracts, which are extremely difficult to negotiate, as they are adhesion contracts.

The issue of liability is also set to become increasingly important with the agentification of AI. Since an agent is now programmed to make decisions and execute actions, many questions will arise: Is an AI agent legally authorized to do this, and who is responsible for any harm that might occur in this scenario?

Here again, it is understood that legal uncertainty may exist, but it hinders innovation should no longer be accepted.

[48] Not to be confused with data lakes, which aim to pool data from multiple stakeholders. A data space is a trusted data ecosystem, consisting of an infrastructure for pooling and sharing data between peers, and dedicated governance. These spaces are necessary for the creation of a single European data market.

[49] General Court of the EU, 29 January 2025, joined cases T-70/23, T-84/23 and T-111/23.

THE RISK OF THE ACCUMULATION OF LEGAL FRAMEWORKS

Beyond the articulation of dedicated texts, the accumulation with other sectoral regulations is also a point of high vigilance.

The health sector is another perfect illustration of these challenges linked to the ex- lack of standards.

Let's take a startup in the sector created in France and proposing to use AI to address a given problem. Obviously, the AI Act and the GDPR come first: is the intended use prohibited or high-risk? Can the required data be used, and under what conditions?

Next come the rules on medicines and health products. The company will have to comply with the regulation relating to medical devices[50] then it will have to comply with the standards of the dedicated Agency in France[51] and those of the agencies dedicated in other countries in which it would like to develop its solution.

The hosting of health data will follow the same, sometimes complex, pattern with required certified servers that will often differ from one country to another, including within the European Union.

It is therefore this proliferation of rules and requirements specific to each sector and country that ends up posing significant challenges, particularly in highly regulated sectors such as healthcare. Security and defense could also be cited.

While the AI Act and the GDPR are often false culprits and offer welcome protection that creates added economic value, contrary to the prevailing discourse, better regulatory integration within the EU is nevertheless necessary to prevent the complexity arising from the accumulation of rules from hindering competitiveness and innovation and to ensure that companies can definitively transform the challenge of regulation into a major competitive advantage.

In this context, mastery of the law will necessarily become an important competitive tool, as will the ability to influence future regulations, in particular by using parliamentary evaluation work.

B. DATA AND USAGE SECURITY AS A CONDITION FOR RETAINING ITS POSITION ON THE MARKET

In addition to the rules of ethics, a second set of rules specific to the news technologies naturally affect AI: cybersecurity rules.

[50] General Court of the EU, 29 January 2025, joined cases T-70/23, T-84/23 and T-111/23.

[51] General Court of the EU, 29 January 2025, joined cases T-70/23, T-84/23 and T-111/23.

Two issues should be particularly mentioned:

- The risks of cyberattacks targeting AI systems,
- The use of an AI system for criminal or tortious purposes.

The latest annual report on cybercrime, published in July 2024 and covering the year 2023, reports 278,770 digital attacks recorded in France in 2023, i.e. a 40% increase in attacks in 5 years, including 59% attacks on property and 6% attacks on institutions and public order.

An infographic published by Bpifrance with a start-up specializing in insurance, Dattak, in April 2024 specifies, with regard to companies, that the number of attacks has increased for 23% of them, that 49% of cyberattacks achieve their objective, and that for 65% of affected companies, cyberattacks have had consequences on their business.

For businesses, cyber risk has become the number one risk in many countries[52].

What's new: **90% of denial of service attacks are carried out using artificial intelligence**, and generative AI enables new "sophisticated attacks" and targeted, at high speed and on a large scale"[53].

1. The emergence of new threats

Disruptive technologies, such as artificial intelligence (AI), particularly generative or agent-based, are being widely adopted by businesses due to the promises of efficiency, competitive advantages, and sustainable business growth they appear to offer.

A study by insurer Hiscox on cyber risk management published in October 2024[54], for example, reveals that generative AI is already integrated into the operations of seven out of ten companies. Yet, only 56% of executives believe this technology will have a significant impact on their cybersecurity risk profile.

This rapid adoption can lead to vulnerabilities if cybersecurity measures do not keep pace: a service can be made unavailable while a company has become totally dependent on it – thus **ChatGPT has already been the target of attacks, including a major one in 2023**[55], an attack can infect the service by poisoning the data[56] or can allow a very large amount of data to be collected, sometimes of great confidentiality.

However, **70% of companies surveyed** for the Hiscox **report say they have already integrated generative AI into their operations**[57].

However, this rapid adoption of new technologies comes with increased cybersecurity risks. Information systems are becoming more complex and interconnected, **increasing companies' attack surface and vulnerability to cyber**

[52] Rapport d'Allianz, « Allianz risk barometer 2024 », janvier 2024.

[53] European Union Agency for Cybersecurity, in the infographic published by BpiFrance and Dattak on April 19, 2024.

[54] Hiscox Observatory, "Hiscox 2024 Cyber Risk Management Report: Cyber Resilience to Protect Reputation," October 24, 2024.

[55] https://www.lesechos.fr/tech-medias/intelligence-artificielle/chatgpt-victime-dune-cyberattaque-massive-2027843

[56] https://fr.blog.barracuda.com/2024/04/03/generative-ai-data-poisoning-manipulation

[57] Hiscox Report, p. 2.

threats. Despite this, only 56% of executives believe technology will have an impact on their risk profile,[58] which may lead to a significant underestimation of potential threats.

This risk is also increased because AI, whether generative or not, exploits a set of pre-existing technologies, which are themselves already at risk.

This is the case of the cloud, another area where the threat is evolving rapidly, and which is the subject of a recent threat report from the French National Agency for the Security of Information Systems[59].

Cloud environments are increasingly targeted by cyberattacks due to the growing interest in the data they process and their role as a potential gateway to organizations' systems. Attackers exploit vulnerabilities in edge devices, such as VPNs, as well as bad configurations and security flaws. These attacks are often motivated by profit, espionage, or destabilization goals. Attackers now use the cloud as infrastructure to store malicious code or stolen data, making the detection of malicious activity more complex.

The SecNumCloud[60] qualification, a label defined by ANSSI, aims to respond to this challenge by specifying the characteristics that a cloud computing service must meet to ensure technical, operational and legal security requirements .

INVESTMENTS IN CYBERSECURITY AND CYBER-RESILIENCE

Insurer Hiscox's 2024 Cyber Risk Management Report highlights the growing importance of cyber resilience for businesses in the face of evolving threats. According to the report, 67% of businesses reported an increase in cyberattacks over the past 12 months, and the average number of cyberattacks experienced by businesses increased from 63 in 2022/2023 to 66 in 2023/2024.

The impact of cyberattacks on corporate reputation is also significant. 61% of executives believe that reputational damage due to a cyberattack would cause major harm to their business. Additionally, 47% of businesses found it more difficult to attract new customers after a cyberattack, and 43% lost customers.

Companies allocate an average of 11% of their IT budget to cybersecurity, and 85% of executives surveyed report investing in cybersecurity training for remote employees. These investments demonstrate that companies are taking the threat of cyberattacks seriously and are seeking to strengthen their resilience.

Cyber resilience is considered very important to the overall business strategy of 74% of companies. However, 53% of companies believe their cyber resilience has improved over the past 12 months, but 40% still rate it at a “basic” or “inconsistent” level of maturity.

[58] Hiscox Report, p. 2.

[59] ANSSI, “Cloud sector – State of the IT threat”, February 20, 2025.

[60] The qualification is based on the ISO 27001 standard.

2. Our legal framework as a competitive advantage

Faced with the challenge of cyber threats, France and Europe have a significant legal framework. This regulation must be seen as a strategic lever for business competitiveness and security.

75% of respondents to a study conducted by the American software company Splunk[61] believe that **business partners appreciate the level of protection offered by Europe, and 68% consider these regulations to be a competitive advantage.**

According to the same study, French companies appear to be better protected against cyberattacks compared to the global average. Only 44% of them reported having suffered a data breach (compared to 52% globally), 40% a ransomware attack (compared to 45%), and 37% a denial of service attack. This performance can be attributed to better adherence to European regulations, which provide a robust framework for cybersecurity.

GENERAL MEASURES OF THE GDPR AND THE AI ACT

The GDPR has specifically raised the requirements for the security of personal data, which is at risk of malicious use by those who retrieve it. The regulation has thus strengthened the security obligations of companies and administrations by providing for the implementation of technical and organizational measures to secure data, the maintenance of a data breach register, the performance of an impact analysis for sensitive processing, the notification to the CNIL of a data breach when it presents a risk to individuals, and the information of individuals of a data breach in the event of a high risk for these individuals.

In 2023, 4,668 data breach notifications were made, 60% of which concerned acts of computer hacking, including 1,006 involving a ransomware attack (22% of the total).

Public administrations are the most affected (18% of the targeted actors), ahead of scientific and technical activities (14%), financial and insurance activities (12%), and human health and social action activities (12%). Over the five years since the GDPR came into force, the public sector thus concerns 22% of notifications, while SMEs represent 39%.

Also, the CNIL notes in its latest report a significant increase in notifications linked to a loss of integrity, i.e. an illegitimate modification of data, and availability, i.e. data made inaccessible for a certain period of time.

Similarly, the AI Act sets out a number of cybersecurity requirements. Seven main categories of requirements can be identified: human oversight[62], risk management[63], security by design[64], documentation[65], data governance[66], record keeping[67], and resilience[68].

The text identifies a type of AI with a very specific risk: general-purpose AI[69]. While increased transparency requirements are planned for these systems, this is also the case for cybersecurity. Like high-risk systems, they must provide an appropriate level of protection and physical infrastructure protection.

[61] Splunk, "Annual Cybersecurity Report," April 2024.

[62] Article 14 of the AI Act

[63] Article 9 paragraphs 1, 2 and 5 of the AI Act..

[64] Article 9 paragraph 5 and Articles 15 paragraphs 1 and 4 of the AI Act.

[65] Article 11 and Article 13 paragraphs 2 and 3 of the AI Act.

[66] Article 10 paragraphs 2 to 5 of the AI Act.

[67] Article 12 paragraphs 1 to 3 of the AI Act.

[68] Articles 14 paragraph 4 and 15 paragraphs 4 and 5 of the AI Act.

[69] As a reminder, these are AIs that exhibit significant generality and are capable of competently performing a wide range of distinct tasks.

DEDICATED TEXTS:

Resilience Directive (REC), Network and Information Systems Security Directive[70] *(NIS2) and Digital Resilience Regulation for the Financial Sector*[71] *(DORA)*

Three texts should be mentioned. Together, they are the subject of a draft transposition law, in the case of the two directives, and of adaptations, in the case of the regulation, currently being examined by Parliament[72]. It should be adopted by the summer of 2025.

REC[73] **Directive**. The directive on the resilience of critical entities aims to improve the resilience of critical infrastructures in 11 sectors.[74] It thus imposes common rules on all Member States in order to guarantee minimum protection. This directive is not, however, new, as it concerns France, which has already implemented a system for identifying operators of vital importance since 2006.[75] It will therefore ensure fairer competition between the operators concerned at the European Union level, with strict but common rules.

This system is based on **shared responsibility between the State and operators**, who must guarantee the **physical and cyber security of their infrastructure**. A new status of "critical entity of European importance" is also created for operators operating in at least six Member States.

NIS Directive 2[76]. The NIS 2 Directive **aims to strengthen the protection of businesses and administrations against cyber risks.** It thus expands the scope of covered entities to 15,000 in France compared to 500 under NIS 1, and now covers 18 sectors[77], which includes local authorities given the increase in cyberattacks against local public services. Entities are classified into two categories: "essential" and "important." This results in proportionate security obligations, which may lead to increased penalties **in the event of non-compliance.**

DORA[78] **Directive**. The DORA Directive concerns the digital resilience of the financial sector and imposes new requirements on financial institutions to prevent digital risks. This regulation thus harmonizes the rules for managing information technology risks in the banking and financial sector.

This legal framework forces companies to anticipate, through risk governance logic, based on the risks identified in data or in businesses:

- By identifying procedures that make it possible to limit risks and resolve future problems,
- By preparing the company for critical scenarios with a strong focus on resilience and the ability to resume activity, including reduced activity, while the problem is resolved as a whole.

The texts outline the mechanisms that will then be activated during crisis management by the steering and crisis management committees, to support

[70] Network and Information Security.

[71] Digital operational resilience Act.

[72] Bill relating to the resilience of critical infrastructures and the strengthening of cybersecurity, tabled on 15 October 2024 in the Senate.

[73] Directive 2022/2557.

[74] Public administrations, drinking water, wastewater, energy, space, management of information and communication technology services, financial market infrastructures, digital infrastructures, health, banking sector, transport.

[75] Vital Activities Safety Device (SAIV).

[76] Directive 2022/2555.

[77] Highly critical sectors: public administration, drinking water, wastewater, energy, space, information and communication technology services management, financial market infrastructure, digital infrastructure, health, banking, transport. Other critical sectors: manufacturing, production and distribution of chemicals, digital suppliers, waste management, manufacturing industry, food production, processing and distribution, research, postal and shipping services.

[78] Directive 2022/2554.

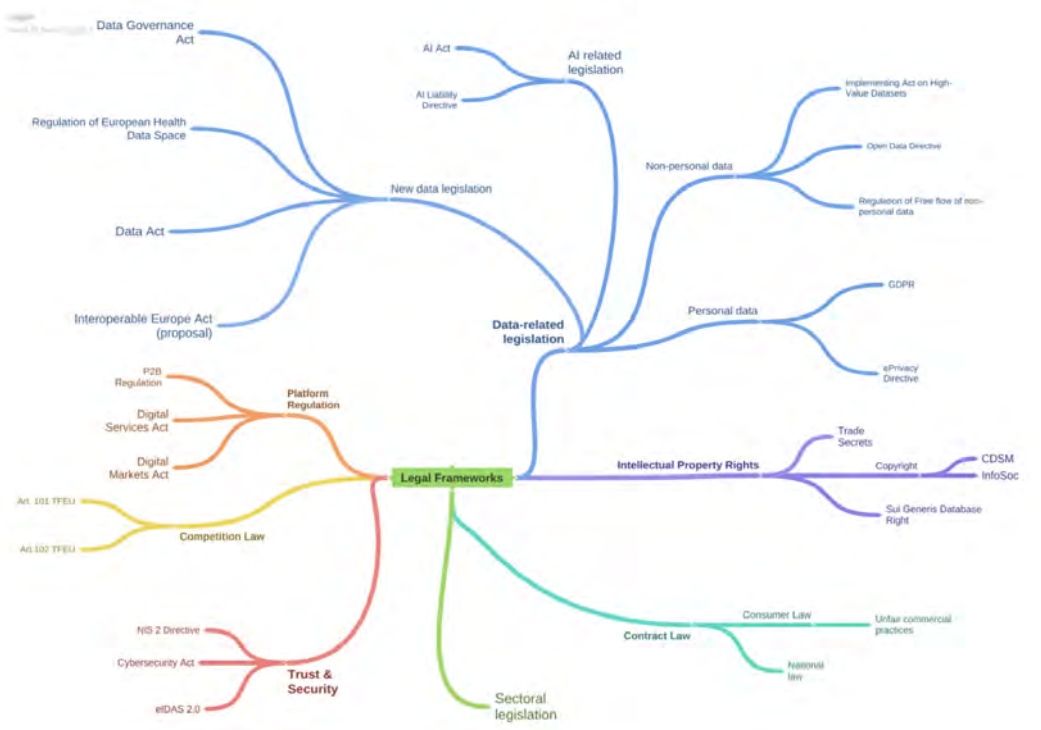
stakeholders from the early stages of an incident with internal notification actions and with those who may find themselves victims – in the context of the theft of personal data from a company's customers, for example.

The legal framework will also help anticipate liability in the event of negligence and thus facilitate future pre-litigation or litigation actions, as well as the criminal aspect, with the filing of a complaint. However, even filing a complaint requires a certain amount of anticipation because it must be done within 72 hours of the incident, otherwise the insurance will no longer be able to be used.

What the legal framework will also allow is to manage contracts with external service providers, both to anticipate the risk, therefore, but also to limit it.

The DORA regulation concerning the financial sector is interesting in this respect because it requires ensuring that security requirements are properly respected by service providers, which may require significant consolidation on the contractual side. Following this work and in-depth audits, this will help to consolidate an environment and ecosystem that complies with the regulations and is therefore more robust.

A LEGAL FRAMEWORK FOR AI THAT GOES BEYOND DIGITAL RULES



Source: DSSC, relevant EU Legislations, November 2024

Beyond the rules dedicated to innovation, numerous legal frameworks initially created out of context can intervene in the deployment of AI. These rules are numerous and sometimes difficult to identify, yet they can, on their own, constitute sufficient obstacles to ruin the value of a model or force a radical change of model.

LAW IS NOT THE ENEMY OF INNOVATION. IT IS THE GUARANTEE OF ITS GENERAL INTEREST.

II. LEGAL INNOVATION TO STAND OUT AND SUPPORT SUSTAINABLE INNOVATION

These rules are of two kinds:

- **all general and cross-cutting legal frameworks,** such as competition law, social law, contract law or intellectual property law. Bodies of rules can obviously be identified but their application to an activity will vary depending on the sector considered.
- **legal frameworks relating to new issues,** which also have significant cross-cutting implications. These include rules relating to environmental protection and human rights, including the duty of care and sustainability legislation.

A. PROTECT WITHOUT SLOWING DOWN: TRADITIONAL LEGAL FRAMEWORKS AND THE CHALLENGE OF AI

The rapid development of AI and in particular of generative AI and then of its agentification, has major effects on different areas of law.

Technology can significantly destabilize the relationship between employees in a company.

business and their work, calling for social rights mechanisms.

The creation of texts, images or music by a machine first calls into question substantially the rules of intellectual property on the profession.

The computing power held by a small number of actors and the need to create alliances to even survive is shaking up the law of competition.

All of this then has massive repercussions on contracts which must take into account new issues, anticipate problems that are sometimes difficult to identify, and create new balances between the parties.

To this must be added sectoral rules, in banking and finance for example example, but also in health and safety.

RISK THAT CAN BE FATAL

It is necessary to identify from the beginning of a project, and at each of its major changes, the legal frameworks likely to be impacted by the developed model. To anticipate the already existing law that it might be tempting to apply there-to apply, on the one hand, and, above all, to provide a clear strategy to prevent an existing or future rule from having consequences on a model under development.

This time it is less a question of using rules to one's advantage than of using

legal technique to create a market and develop it without fear of seeing it invalidated by the standard afterwards.

Three scenarios that can lead to the worst must therefore be avoided:

• **A regulatory or legislative change that significantly constrains the company-taken, or even the force to modify the model.**

Recently, players in digital object games have felt the effects of this. As online games developed, modeled on the famous Panini albums of our childhood, but with cards convertible into cash, the players in the gambling industry, a largely regulated profession, forced policymakers and legislators to question their legal framework. In this context, it was necessary to resort to legislation to provide for an experiment.

The SREN law creates this regime by establishing a legal definition of JONUM and providing for its applicable regime with player protection measures, strict rules for the sports and horse racing sectors, and supervision by the National Gaming Authority. The problem is that the proposed regime regulates the activity well beyond the self- regulatory mechanisms provided by the players, and for example reduces to next to nothing the winnings convertible into cryptocurrencies, thus reducing part of the attractiveness of these games.

• **Too much complexity given unsuitable rules.**

This could be a similar case to the one mentioned above in the health sector, with the interweaving of rules specific to digital and rules specific to the health sector, then the accumulation of standards that differ from one market to another, but which have nevertheless worked and protected a physical economy for many years.

• **Non-compliance due to the application of a rule that was not anticipated or was poorly anticipated.** Intellectual property is a good example of this.

The case of the startup Ross Intelligence is interesting in this regard. In February 2025, a US court found the startup guilty of using content produced by a Canadian subsidiary of the Thomson Reuters group to train an AI in the field of legal information. The startup's lawyers attempted to demonstrate «fair use» of protected works.

However, the court found that Ross's AI, which has since shut down, was not generative and that for each response, pre-written opinions were proposed, which were retrieved directly from the Thomson Reuters subsidiary in question. **The lack of transformative value therefore ruled out the notion of «fair use.»**
Three other similar cases are ongoing[79], each with extremely high financial stakes, since American law provides for a fine of up to $150,000 for each violation found. The nature of AI, whether generative or not, could have a major impact on the solutions proposed. However, the three companies defending the case are not yet saved, because in the Ross case, the judge also specified that fair **use should be excluded when the content used serves to offer alternatives to the original services** (creating an image instead of buying one, for example), or when the use of the data

[79] Getty Images stock photo bank vs. British startup Stability AI, The New Times vs. OpenAI, and the RIAA which represents the American recording industry against the song creation AIs Udio and Suno.

had a significant effect on a potential market, **in other words, if it prevents rights holders from monetizing their content from AI designers.** Two characteristics that do not appear to be excluded in the cases in question.

1. Social law and the issue of internal membership

Many companies are tempted to deploy AI solutions, particularly to improve customer service or increase efficiency, both in terms of time and quality. This is true regardless of the sector: manufacturing, mass distribution, or retail.

Thus, in 2023, the Carrefour brand deployed three AI solutions: a robot advisor called Hopla for online shopping, a generative AI to improve product sheets posted online and another generative AI for internal processes. Leclerc brands have equipped themselves with the Captana solution which uses AI and computer vision to report stock shortages in real time and avoid stockout rates[80].

At the same time, several industries have optimized their production lines thanks to the OPTIMAI[81] project, which helps eliminate errors from manufacturing processes.

Since the legal challenges are being discussed, the first instinct is to return to the rules on data, then on usage, and possibly to discuss liability in the event of a solution failure. A recent order from the Nanterre Judicial Court, however, opens the discussion to employment law.

In 2024, insurer Metlife France is rolling out no fewer than five artificial intelligence projects: a tool to combat document fraud, a generative AI for video, another for a CRM, a third for text and images, and an internal chatbot. Although presented as pilot projects, all will be offered to employees reporting to the Director of Operations on November 20, 2024.

Shortly after, the company's Social and Economic Committee (CSE) took action in summary proceedings to block the deployment, for failure to give its opinion.

However, the labor code is very clear: "*The works council is informed and consulted, prior to any major project to introduce new technologies, when these are likely to have consequences on employment, qualifications, remuneration, training or working conditions.*[82]"

The CSE thus raised questions about the possible increase in the workload linked in particular to the solution for combating document fraud, and about the risks of job losses in the event that the tools deployed would make it possible to increase productivity with fewer human resources.

Whereas it is irrelevant whether consultation with the CSE is mandatory or not, the Nanterre judicial court ordered, as a matter of urgency, the halting of the deployment of the five projects in question, pending the end of the CSE information procedure, with a penalty payment of 1,000 euros per violation per day.[83]

[80] According to VusionGroup, which produces the solution, initial in-store trials have reduced the stockout rate by 3%.

[81] Optimizing Manufacturing Processes through Artificial Intelligence and Virtualization.

[82] Article L2323-29 of the Labor Code.

[83] Nanterre Judicial Court, interim order, February 14, 2025, no. 24/01457

While the AI Act establishes a general obligation to train personnel affected by AI systems[84], the order of the Nanterre judicial court, although issued urgently and therefore without a final judgment on the merits, forces us to consider labor law in a different way than just through training.

Obviously, not all projects are subject to these rules. However, it would be good practice to add labor law rules to the project analysis software whenever it concerns a company that needs to establish a CSE[85].

Otherwise, the deployment of the projects could be significantly delayed and, above all, their acceptability would be called into question, possibly leading to their abandonment given the protests raised.

2. Intellectual property law challenged by generative AI

Aside from rules dedicated to digital technology and artificial intelligence, legal frameworks relating to intellectual property are certainly among the most cited, since the rapid emergence of generative AI: who is the author and the holder of the rights to an AI production? Can we exploit and/or protect content generated by AI? How can we ensure compliance with the underlying rights that would belong to the authors of the sources potentially used, particularly in the learning phase?

To provide a rough answer, it's first important to clarify how AI works to avoid any misunderstandings. Generative AI creations are often misunderstood when it comes to their development. Some consider that content generated in this way is only a reproduction of a original, therefore systematically searching for the source to then pull the thread of classic intellectual property rights linked to reproduction.

The principle of generative AI is to learn from a machine learning model and then create content autonomously, just as human intelligence would. That is, it's not about retrieving pieces of data and reusing them in whole or in part, but rather creating new, completely original content.

Where original content ultimately comes into play is in the learning phase. Just as a painter regularly wanders through collections of works or the aisles of a museum to draw inspiration from them, a generative AI first learns from existing works before creating its own. Beyond the works, the learning data could also contain stories from artists or analyses of their techniques, to identify the best methods.

And it is precisely in this complex mechanism, similar to that of human intelligence, that the rules of intellectual property are challenged.

This is a challenge, however, not unfamiliar, as it largely recalls recent cases involving entirely human intelligence, this time. This is the case, for example, of Gad Elmaleh, who was accused of plagiarizing some of his sketches. At what point does a comedian move from inspiration to plagiarism?

[84] Article 4 of the AI Act.

[85] Article L2311-2 of the Labor Code: "A social and economic committee is set up in companies with at least eleven employees. Its establishment is only mandatory if the workforce of at least eleven employees is reached for twelve consecutive months."

These topics are ultimately nothing new and go far beyond comedians. One only has to listen to the few trumpet notes in Shakira's «Hips Don't Lie» after listening to Jerry Rivera's «Amores Como El Nuestro,» which the Colombian singer had absolutely no warning about, to be convinced.

Rather than rushing into uncharted territory by getting so close to the functioning of human intelligence, with a learning phase followed by creation, generative AI has finally moved towards more familiar problems.

When doubt arises regarding the possible use of elements produced by an author without prior authorization, **the question would ultimately be the originality of the content created in relation to the training data**. Just as the legality of a Gad Elmaleh sketch will depend on its originality in relation to the sketches that may have inspired it, or that of trumpet notes to make Shakira and her fans dance will depend on their originality in relation to notes from another trumpet that had already made a good part of South America dance.

What is disturbing, basically, is that it is no longer a question of judging the creation of a peer but of a machine, and this on an unprecedented scale and with a risk of perpetual repetition. What is also disturbing, and perhaps most of all, is that the artist has usually gone to a school or purchased past performances to learn.

But this time, it would be possible to learn without having purchased anything, without any form of financing for creation. With the risk of breaking a virtuous circle, which pays as much as it finances art and thus our culture and that of others.

This is also a question of sovereignty.

Two main issues then emerge:

- On the one hand, the importance of finding the right mechanisms to enforce property rights and share value without blocking innovation.

A 2019 directive on copyright and related rights[86] provided for an exception to the rules on the use of protected works and other subject matter for text and data mining[87]. This rule allows, in practice, the use of even protected content as long as it is freely accessible on the internet. An exception to this exception is provided if the use of protected works and subject matter has been *"expressly reserved by their rightholders in an appropriate manner, in particular by machine-readable means for content made available to the public online"*[88] (opt-out principle).

Although the principle seems difficult to dispute, its implementation is not simple since it will be particularly difficult for an author to know whether his work has been used or not.

To address this difficulty, the AI Act introduced transparency requirements for developers of general- purpose AI models to ensure the traceability of data and

[86]Directive 2019/790.

[87]Article 4 of Directive 2019/790.

[88]Article 4, 3 of Directive 2019/790.

content, and to inform users and those whose content is used[89]. This summary must sufficiently detail the content used to train the general- purpose AI model[90].

The level of content in this summary requires careful consideration; it's about striking a balance between copyright protection and innovation. If all the elements relating to the learning data were included, this would amount to revealing all the techniques for a comedian or a trumpeter.

A report commissioned by the Higher Council for Literary and Artistic Property from Professors Alexandra Bensamoun and Joëlle Farchy is to produce proposals on this subject during 2025.

In this regard, we could, for example, assess the possibility of implementing a mechanism for distributing the value created based on the role played by training data in the creation of content by an AI generative[91] based on a data space of cultural actors.

- On the other hand, the need for sovereign solutions to ensure that culture is not guided solely by American or Chinese sources, to the point of ultimately abandoning what has partly been the pride of France and Europe.

3. Competition law and barriers to entry to AI

Among the issues that must be considered alternately by AI developers and those deploying them, competition law also figures prominently. Namely, the prohibition on companies colluding with competitors or business partners to restrict competition, or taking advantage of a market position to abuse it to the detriment of a competitor.

The emergence of AI, and even more so generative AI, is disrupting business models: from improved performance, to the ability to integrate activities initially carried out at another level of the value chain, to the creation of new services to capture more market share.

The topic of generative AI was the subject of a very comprehensive report by the Competition Authority, published in June 2024, as proof of its growing importance. This report addresses in particular the issues of cloud computing, including those related to access to these infrastructures, computing power, data and a skilled workforce, as well as the equity investments and partnerships of major digital players in the generative AI sector.

The Authority proposes three main findings:

• **High barriers to entry.**

First, because deploying generative AI requires rare computing power for both

[89] The initiative of Jeremy Howard, an Australian data scientist, can be highlighted in this respect, since he offers the tech community a standard for coding rules for sharing intellectual property rights, understandable by crawlers. For a concrete example, see: https://docs.anthropic.com/llms-full.txt.

[90] Article 53, 1. d) de l'AI Act. Ce résumé doit être conformé à un modèle fourni par le Bureau de l'IA, qui doit par ailleurs encourager et faciliter l'élaboration de codes de bonne pratique, comprenant notamment le niveau approprié de détail pour ce résumé (article 56, 2. b) de l'AI Act).

[91] A model of this type, entitled "Hugging Face Space" is proposed by TheFrenchDemos and could serve as a starting point.

training and tuning and using the models, and significant legal expertise. As a result, very few players are able to offer these services[92], which only increases the costs.

Then, cloud computing appears essential as does the fact of have large volumes of data.

Finally, technical skills are scarce and the need for financing is significant.

In this regard, the authority mentions three **developments likely to remove some of these barriers: public supercomputers** which would be used free of charge in exchange for a contribution to open science, **technological innovations** which would reduce the need for computing power and data[93], and **open models.**

In addition to these avenues, the future of public-private partnerships must also be questioned, in a context where European rules on state aid are not very favourable to them.

- **A risk of competitive advantages for major players** in other markets on which the development of generative AI is based.

Thus, large digital companies necessarily have an advantage in terms of elements necessary for the development of generative AI: computing power thanks to preferential agreements with their historical partners, privileged access to a large volume of data, technical skills attracted by salaries.

They also benefit from economies of scale and network effects. Their historical activities allow them to feed AI to refine models or define new services. Also, the integration of generative AI tools into initial products provides a clear advantage in terms of market acquisition. **This is the case, for example, when Microsoft deploys its models and those of OpenAI in the «Copilot» tool,** with which it has signed a partnership in the form of a multi-year investment.

Their marketplaces are also a significant asset since they assure large digital companies that a large number of models will be designed to work in their ecosystem.

- **Competitive risks at the beginning of the value chain.**

Several risks are thus identified by the Competition Authority: risks of abuse at the level of IT components, **risks of lock-in** by large cloud computing service providers, risks linked to refusals of access or discrimination in access to data, risks linked to no-poaching agreements between companies in the sector, risks linked to open access models when they lead to user lock-in, risks linked to the presence of companies in several markets given the vertical integration of certain players and which could lead to refusals or limitations of access to elements essential for training competing models, risks linked to minority shareholdings and partnerships by large digital companies as confirmed again by the partnership between Microsoft and OpenAI, and risks of collusion in the event of the use of generative AI which would create concerted practices.

Aware of the challenges facing the sector, the Competition Authority also

[92] Graphics processors developed by Nvidia are, for example, in extremely high demand, with few alternatives possible.

[93] In this respect, the Chinese AI Deepseek has been able to raise hopes given the information revealed on its cost and the absence chips developed by Nvidia. However, this information could not be verified at this stage.

published a consultation in January 2025 to gather market opinions on the possible introduction of a merger control system for transactions falling below the merger notification thresholds. This would entail all the difficulties in qualifying markets that this would then pose.

In this respect, the regulator will necessarily be confronted, in the coming months, with practices which, while they aim to overcome all or part of the difficulties identified cultures, in turn create challenges in terms of competition law.

This is the case, for example, of sectoral data spaces, also called *data spaces*[94]. These spaces make it possible to create systems with significant added value, and thus overcome the already real hegemony of certain actors, who do not have data of such quality by sector.

However, the way this data is shared and the nature of the generative AI that is then created to use it can create new barriers, particularly for smaller players who would not be able to benefit from useful information for the development of their activities.

Given the strategic importance of these models for the sovereignty of France and Europe, it will be necessary to work hand in hand with the regulator to overcome any obstacles.

B. RETHINKING THE USE OF SUSTAINABILITY RULES TO PROMOTE EUROPEAN- STYLE AI

Sustainability, understood as the ability of a technology to last over time, is very regularly cited as a major challenge for AI, particularly generative AI. This concern is often linked to the figures cited regarding the models' consumption: a query made from ChatGPT would consume more than 10 times more electricity than a classic Google search, according to the International Energy Agency, which also predicts that electricity demand for data centers is expected to more than double by 2026 compared to 2022 figures.

AI AND VOLUNTARY SUSTAINABILITY

Yet a simple search within the AI Act brings up only four occurrences of the term "sustainability":

- in the recital, suppliers and those deploying AI systems are encouraged to apply on a voluntary basis additional requirements related, in particular, to "environmental sustainability"[95] ;
- this recital mirrors an article on codes of conduct for the voluntary application of certain requirements, which mentions *"assessing and minimising the impact of AI systems on environmental sustainability, including with regard to energy-efficient programming and techniques for the efficient design, training*

[94]Reminder of the definition: trusted data ecosystem, composed of an infrastructure for pooling and sharing data between peers, and dedicated governance. These spaces are necessary for the creation of a single European data market.

[95] Paragraph 165 of the recital of the AI Act.

and use of AI"[96] among the objectives whose achievement should be facilitated by the development of codes of conduct.

- these two provisions are also followed by a mention in the article relating to the re-evaluation and re-examination of voluntary codes of good conduct, in that they must promote the application of requirements including environmental sustainability[97].
- in the article relating to the regulatory sandbox, "*AI systems (…) developed to preserve important public interests by a public authority or another natural or legal person (in matters of) energy sustainability*[98]" are among the cases mentioned to be able to benefit from it, subject to compliance with the other conditions;

No hard and fast rules are actually planned, specifically regarding digital or AI, whether generative or not.

1. Concrete sustainability mechanisms already in action in large companies

Our companies can already rely on known mechanisms, which most of the largest of them already respect: **the duty of care and social and environmental criteria.**

These rules have recently been thrust into the news because they are the target of simplification measures proposed by the European Commission, as part of the so-called "Omnibus" procedure.

The duty of vigilance appeared in French law by a law of 2017[99], requiring companies with more than 5,000 employees in France or more than 10,000 employees worldwide to take "*reasonable vigilance measures to identify risks and prevent serious attacks on human rights and fundamental freedoms, the health and safety of people and the environment, resulting from the activities of the company and those of the companies it controls (…), directly or indirectly, as well as the activities of subcontractors or suppliers with whom an established commercial relationship is maintained, when these activities are linked to* this relationship."[100]

Since then, the duty of care has been applied to around 300 companies in France. Its European version, the CS3D directive *(Corporate Sustainability Due Diligence Directive)*, was to be applied between 2027 and 2029, with an expanded scope, extending to more than 700 companies in France. On February 26, the European Commission announced that this due diligence obligation would ultimately only apply to direct business partners, that the frequency of assessments would increase from one year to five years, and that civil liability conditions would be removed. This latest announcement is certainly the most significant since it removes almost all force from the directive's obligations.

[96] Article 95, 2, b) of the AI Act.

[97] Article 112, 7 of the AI Act.

[98] Article 59, 1. a) of the AI Act.

[99] Law No. 2017-399 of March 27, 2017 relating to the duty of care of parent companies and contracting companies.

[100] Article L. 225-102-4 of the Commercial Code.

At this stage, however, this step backwards at the European Union level has no effect on the French duty of care, nor that applied in other Member States in recent years, such as in Germany where the thresholds are, moreover, significantly lower[101].

The other important body of rules regarding sustainability is contained in the CSRD *(Corporate Sustainability Reporting Directive)*, transposed into French law by an order of December 6, 2023[102], it is also carried over and very largely amended by the omnibus package presented by the European Commission. This directive expands transparency obligations regarding sustainability, by requiring companies to detail how their activities have an impact on the environment and society, and how risks and opportunities in terms of climate transition and social responsibility are managed.

At the French level, Parliament will examine in spring 2025 the conditions for the postponement of sustainability rules, in accordance with European announcements. Thus, at the beginning of March 2025, the Senate adopted an amendment to allow large companies and consolidating companies to start reporting in accordance with the CSRD directive for the year 2029, small and medium-sized enterprises to do so for the year 2030 and non-European small and medium-sized enterprises for the year 2032.

2. Transform compliance into a lever for managing risks linked to AI

Compliance can be expensive—between collecting supply chain data, analyzing impact, and implementing controls—and is clearly not a priority for most startups. The standards are complex, and their articulation isn't always straightforward.

Once implemented, the added value of these rules for the companies that adhere to them is often barely perceptible and casts doubt on their appeal in a globalized market, compared to companies that have little to do with sustainability. Thus, companies from all over the world, and especially from China and the United States, could concentrate all their resources on technological and commercial development, while our companies would be forced to sacrifice part of one or the other, or a little of both, without knowing what the point would be.

At first glance, these rules therefore have few advantages. However, mentioning these rules seems essential for at least three reasons:

- the lack of risk management in terms of sustainability can only be short-term, when it comes to AI, given its environmental and human rights characteristics,
- a portion of large companies likely to have the resources and perspectives necessary to deploy AI solutions are subject to it ties in whole or in part,
- AI can be a formidable tool for addressing transition issues, but is only viable as such if its own characteristics are compatible with this objective.

Regarding the first point, a recent report from the Capgemini research institute assesses the entire resource consumption of the generative AI value chain and

[101] Article L. 225-102-4 of the Commercial Code.

[102] Article L. 225-102-4 of the Commercial Code.

notes, for example, that training a ChatGPT-4-type model alone requires enough electricity to power 5,000 homes in the United States for an entire year.

The same report mentions that 47% of the companies surveyed consider that their greenhouse gas emissions have increased over the last 12 months, 48% recognize that generative AI is one of the reasons and 42% admit that they will have to review their commitments in terms of sustainability in view of generative AI.

At the same time, only 12% of companies surveyed measure the environmental footprint of this technology and 74% say that the lack of transparency from companies providing the technology makes measurement difficult, acknowledging that they expect the tech sector to drive sustainable generative AI.

This largely explains why, while large companies are already largely subject to sustainability rules, very few are integrating AI issues into them.

Thus, the association "Interest in Acting "[103] published a report in September 2024[104] noting that out of 11 French companies tested, only one had implemented measures related to the deployment of AI, following an investigation it had been subject to in Colombia.

However, AI, and in particular generative AI, intervenes at least on two levels in environmental and human rights issues: first in the context of the extraction of minerals required for the manufacture of electronic components with both human and environmental risks, then in the context of the training and operation of systems with human risks linked to data processing and environmental risks linked to the operation of systems and *data centers*.

While environmental issues are acknowledged, due to a lack of real consideration at this stage, the subject of human rights is often overlooked due to ignorance. The spotlight on data workers in a mainstream context is recent.

In India alone, by the end of 2024, more than 70,000 people were employed to annotate and validate data that would then be used to train models. Among these people, around 50,000 freelancers. With all the precariousness and in certainty that could be noted in the past with regard to the workshops of the world, which are at the origin of the duty of vigilance, since the fall of Rana Plaza, an eight-story building in the suburbs of the capital of Bangladesh, which housed textile workers.

But although the European Union is playing down sustainability for fear of hampering innovation, French rules and those of a number of our European neighbors, led by Germany, are not taking a break.

On the contrary, after some time spent clarifying procedural rules, France is now experiencing its first substantive disputes. A chamber dedicated to emerging disputes has been created in Paris, and the La Poste group was the first to be convicted for failings in due diligence related to respect for workers' rights.

This is where large companies and AI startups must work together. Some have the resources and maturity to work on their sustainability now. Others have the

[103] This association is dedicated to strategic litigation and is part of a group also composed of a fund of endowment, Dotlex, and a think tank, Lex Ferenda.

[104] Baptiste Delmas and Juliette Terrioux, "Artificial intelligence and duty of care, there is an interest in acting", September 2024.

technical information needed to do so.

Obviously, no model is perfect, and viewing the duty of care as a no-fault obligation is not the goal.

It is, above all, an obligation to set an example, to do everything possible to ensure that, ultimately, the environment and human rights—and ultimately, humanity—are not the big losers from technological progress.

These considerations are currently taking a back seat, but they will soon come back to the forefront with the first accidents or scandals.

The usefulness of these rules for our businesses is all the more important since, with nuclear power, we have built the first building block of a very favourable local context. Barclays[105] research teams, for example, have created a map that describes the percentage of time in a data center's operation during which its supply can be provided by decarbonized energy. France thus owes its great attractiveness to a rate of 94%, the second highest in the world behind Finland (98%) but far ahead of Ireland (43%), Italy (52%) and, to a lesser extent, Spain (76%).

But while we benefit from this building block and Europe's pioneering spirit in terms of responsible digital technology, we currently enjoy no market advantage. Worse, we are postponing rules that could make a difference by imposing real constraints on less virtuous foreign players.

The question, ultimately, is how can a common-sense practice in the general interest become a weapon for our companies, both for their business and for the long-term influence of our values throughout the world?

[105] Barclays Research, "AI revolution: meeting massive AI infrastructure demands ", January 2025

OPPOSING REGULATION AND INNOVATION IS TO RENOUNCE SOVEREIGNTY.

III. THREE CONDITIONS FOR MAKING OUR LAW A REAL WEAPON

Our legal arsenal is extensive. And therefore complex. But it reflects the principles of European-style AI: ethical, safe, and sustainable. European-style AI is not a technological advancement; it's a societal project.

To achieve this ambition, it became clear, through the analysis, that certain rules had to be simplified, and that all of them had to be better articulated.

To achieve this ambition, it must also become clear that the law must no longer be a simple translation of our values. Three conditions seem to be necessary for the law to become a weapon. An economic weapon, first, and a strategic and global weapon, second and foremost:

- be a tool to secure and accelerate innovation;
- facilitate the acceptability of innovation on the European market and ultimately help to impose our rules of the game on the rest of the world.
- be able to act against competitors who do not play the game, whether in the context of public or private markets, and in the defense of virtuous models.

A. THE RULE OF LAW AS A TOOL TO SECURE AND ACCELERATE INNOVATION

Legal frameworks are still too often viewed as compliance obligations that only add cost lines. However, the law must facilitate the technical standardization of products built with AI.

The standardization of technology through law must provide guarantees in terms of quality and therefore trust, but also facilitate the work of AI suppliers and deployers, by marking out the path, however tortuous, of innovation.

1. The driving role of law in the scalability of innovation: from cost line to strategic infrastructure

As part of the hearings carried out for the production of a recent report submitted by the Parliamentary Office for the Evaluation of Scientific and Technological Choices (OPECST)[106], Yann Ferguson, sociologist and scientific director of Inria's LaborIA and Patrick Bezombes, Advisor for AI Strategy and Governance at the Association French Standardization Agency (Afnor) and representative of France at CEN-CENELEC[107]

[106] A. Sabatou, P. Chaize, C. Narassiguin, "New developments in artificial intelligence for evaluating scientific and technological choices," November 2024.

[107] European Committee for Standardization in Electronics and Electrotechnology

insisted on the interest of the technical standardization provided for by the AI Act.

Two categories of companies stand out:

- **Traditional** indutrial companies, which are accustomed to strict standardization, which is essential both to guarantee the safety of their products and for the company's reputation. In addition to these two elements, we could add acceptability, which is ultimately just an obvious hat. These companies know that to bring a cruise ship, an airplane, a train, or a nuclear reactor to market, the risk can only be minimal.

A notable example is Boeing, whose stock has fallen by around 55% over the past five years. Analysts have widely lamented the company's prioritization of profitability over engineering, which has led to systemic problems in the management of safety issues, which, coupled with supply chain difficulties, have had significant consequences for its market position.

- **New companies, particularly in the digital sector, which allow themselves higher margins of error** since they have encountered fewer major problems at this stage. The OPECST report also specifies that errors are more tolerated in the sense that they can subsequently be corrected by a simple software update.

Those interviewed on this subject see the AI Act as *"a way to encourage digital companies to change their culture and adhere to strict standards when marketing a product."* Once again, it is a question of acceptability through the trust that a client company or an end customer will feel.

This standardization would also largely offset the cost it would represent for small businesses compared to large ones, since a failure would lead to a loss of confidence that would be just as penalizing for a large business as for a small one.

Also, the simplification system provided for by the AI Act[108] further limits costs with both the application of a principle of proportionality and priorities for access to facilitating infrastructures such as the regulatory sandbox.

Experience has also shown us that the risk of failure is easier to absorb for a large company capable of diversifying its offerings, especially under different brands, than for a large or smaller company dependent on a single product, which has a significantly lower risk dilution capacity.

Using law to standardize innovation has the same advantages in terms of product quality (AI Act) as in terms of data ethics (GDPR)**, cyber standards** (set of directives and regulations, as well as internal rules regarding insurance requirements for example), **cross-cutting legal rules and sectoral, and sustainability standards** (duty of care and communication criteria in particular).

The paving stones are somewhere ready to standardize the path to innovation. What 's missing is a legal infrastructure capable of laying each of them down so that both large companies, accustomed to them, and smaller ones, which have virtually no experience and learned to grow without them, can rely on them.

[108] See below

This legal infrastructure that must be built is the possibility for our companies that provide or deploy AI to develop with less of the burden of compliance but more of the virtues of the rule of law.

2. When Kelsen[109] meets Turing[110] : *Law as an Infrastructure, Law as a Platform, Law as a Service*

Understanding technological specificity through law constitutes an essential prerequisite – as much as understanding legal logic by innovators.

To initiate this dialogue, we propose to bring together the IT infrastructure plan and that of legal standards.

It is a question of imagining through this analogy the existence of a law capable of evolving the extent of the innovations it supports.

LAW AS AN INFRASTRUCTURE (LAAI): APPLYING FREEDOMS AND RIGHTS FUNDAMENTALS BY DESIGN

A first, unalterable layer must be made up of the fundamentals of the legal system applied to artificial intelligence.

These are, on the one hand, fundamental freedoms and rights, which are at the top of the hierarchy of standards: the rights inherent to the human person (including equality, liberty, security, and the rights which are aspects or consequences of these, including freedom of expression), social and economic rights (including the right to employment), and so-called "third generation" rights (including the right of everyone to live in a balanced and healthy environment", which enshrines the notion of sustainable development and the precautionary principle).

The GDPR and the AI Act protect some of these fundamental freedoms and rights.

This layer, as for Infrastructure as a Service, is the one on which everything rests, and which must therefore be both integrated from the start and fixed.

LAW AS A PLATFORM (LAAP): THINKING OF LAW AS A PLATFORM ACCESSIBLE TO MACHINES

This second layer must be available to anyone who wants to use the right to run their systems. In other words, **this layer consists of making the right executable in code**, in the same way that *Platform as a Service* allows services to be built.

If none of the three layers considered is identified as such at this stage, this is undoubtedly the one which requires concentrating the recommendations as it appears strategic and less developed.

Cela implique, d'une part, de faciliter la traduction du droit dans le code, et d'autre part, de s'assurer de la disponibilité et de l'harmonisation des interprétations des

[109] Hans Kelsen (1881-1973) developed the concept of the pyramid of standards which leads to considering all legal standards according to different blocks (constitutionality block, conventionality block, legality block and regulatory block) with a hierarchy between them.

[110] Alan Turing (1912-1954) is regularly considered the father of computing and a pioneer of intelligence artificial.

textes pour faciliter une intégration dans le code.

This would involve proposing a common platform within the European Union:

- With all the essential texts (initially it seems relevant to limit ourselves to the texts relating to data, the AI Act and cyber rules) in a codable version,
- With all the decisions and legal resources relating to these texts,
- Usable in all countries.

Three recommendations can be made in this regard:

Make the code the 25th language of the European Union so that any new text can find a translation in the code. Following on from the reflections put forward by Enrico Letta through his proposal to create a 28th European regime[111] – aimed at simplifying access to the law for businesses by offering them a harmonized and optional legal framework – our initiative to make the code the 25th official language of the European Union is part of a complementary ambition. The idea is that any–,new legislative text must find a direct translation in the form of code, in order to accelerate and automate its practical application. **This 25th language project could build on the European Commission's "Rules as Code" project[112] and thus strengthen, or even supplement, the objective pursued by the 28th regime: simplifying access to the law, guaranteeing its intelligibility and effective implementation** in a digital and cross-border environment. Our proposal thus contributes to laying the foundations of a genuine digital single market for law, consistent with the dynamics driven by Letta and in response to the modernization needs expressed by the European institutions.

Integrate into the omnibuses being prepared at European level modifications to allow the short-term coding of the main texts, in line with the work already started,

Initially, promote the *Legal Data Space* initiative at the French level, which already brings together a large number of players in the legal sector. This is a shared infrastructure for processing and sharing public legal data (open data) and private data (data spaces) with the aim of developing a sovereign legal AI, by and for the legal sector.

This initiative could ultimately provide solutions to other data spaces for managing data rules. Everyone could thus benefit from a right - from positive law to data sharing contracts[113] - that is understandable by machines and translated into a Rulebook[114].

Thus, AI will no longer be an obstacle but a major asset for ensuring compliance among stakeholders[115].

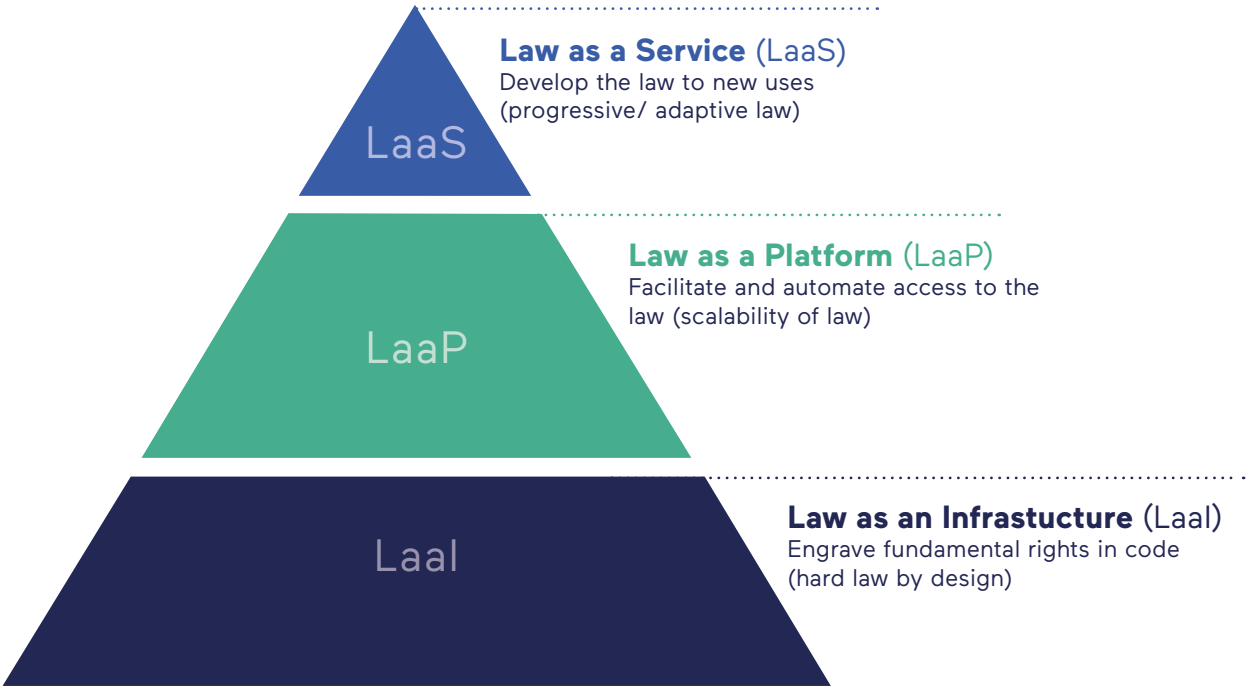
[111] Much more than a market, Enrico Letta, April 2024

[112] https://interoperable-europe.ec.europa.eu/collection/govtechconnect/news/rules-code-rac. In this context, for example, a hackathon was organized on March 17 and 18, 2025 in Paris by the Interministerial Digital Directorate (DINUM).

[113] Thomas Saint-Aubin, Pierre Marchès, "Generative AI and contract management: a revolution underway Heritage, 2024, Generative AI and legal professionals, No. 347.

[114] This approach can be facilitated by the maturity of the European legaltech ecosystem and its digital lawyers, in conjunction with lawyers: Thomas Saint-Aubin, "Digital ethics of lawyers: the duty of exemplarity of legaltech. Ethics in the digital age", Université Cergy-Pontoise, June 2022, Cergy-Pontoise (University of), France.

[115] See on this subject the European Commission's project to use AI to analyze and extract sectoral compliance obligations from current texts and create a new standard which would allow VSEs and SMEs to know natively all the obligations to which they are subject.



KELSEN-TURING PYRAMID
Architecture of law for a European AI

LAW AS A SERVICE (LAAS): MAKING LAW A PLAYER OF INNOVATION

This third layer must provide an agile framework that can evolve depending on contexts, to facilitate ongoing innovation.

This layer is present in the AI Act in the form of "regulatory sandboxes." The aim is to support experiments within the framework of secure regulatory environments.

These sandboxes can be particularly useful in the context of transformative innovations. This is the case with the current advances in AI agentification, which promises to disrupt both the economy and traditional legal mechanisms by allowing AIs to act autonomously, in different contexts, and with objectives, including self-defined ones.

To operate over time, particularly in highly regulated sectors such as health or security, it will be necessary to anticipate all irritants to identify persistent blockages that would require changes to legislative or regulatory rules or rules dedicated to AI systems or data, for example (this could be the case for reimbursement rates in health, or competence rules in security).

A SOVEREIGNTY ISSUE

It is not about replacing the lawyer, the jurist or the auditor with artificial intelligence, but about safeguarding our rules of law in this new world.

Humans will obviously find their place there, and certainly more than at present: firstly, to ensure the conformity of the code, then to deal with any difficulties that arise in the implementation, and finally, to support entrepreneurs with their vision of the legal infrastructure.

On the contrary, **in a scheme where we would renounce the establishment of such a legal layer, we could ultimately see our model overtaken and replaced, in particular by *Common Law***, in certain points easier to use with artificial intelligence.

In particular, because the Common Law system is based on case law, and is thus likely to evolve to adapt to contexts, based on reality. The ability of artificial intelligence to analyze a large number of elements can thus facilitate, based on precedents, logical solutions, and an adaptation of the rule to very specific situations. It is for this same reason that in the business world, already, economic actors regularly favor Common Law.

Our law, based on the Romano-Germanic tradition, on the contrary, exists only because a rule has been set in stone. And case law only clarifies **this rule. This rigidity can make reasoning from the code more difficult** when the rule has not been previously thought out for it.

The danger is all the more pressing as new modes of governance, particularly data governance, develop with common governance rules. This is the case with data spaces. However, if our law is not codable in this area, the risk is that stakeholders may eventually turn to the simplest system.

B. THE RULE OF LAW AS A TOOL OF ACCEPTABILITY AND EXTRA TERRITORIALIZATION OF OUR VALUES

In the study by KPMG Australia and the University of Queensland published a year ago and cited in the introduction, only 31% of French people said they were ready to trust[116] to AI, when 96% considered that the practices and principles of trustworthy AI determine the trust placed in AI systems.

Several studies had already revealed, over the past three years, that consumers were increasingly sensitive to the protection of their privacy and were choosing to use products and services that protect it. Thus, in a study published in March 2022, 80% of French consumers considered the protection of their data by a brand as a key factor in granting them trust. Another study published in July 2022 indicated that 72% of French Internet users were concerned about the recording of their online activities for advertising targeting and 82% limited the provision of their personal data online[117].

1. Facilitate market evangelization through the normative force of law

Also, although ChatGPT has reached in a few months a number of 300 million weekly users that it took eight years for Facebook or four years for Instagram to reach, it should not mask the difficulties that the diffusion of AI faces.

OpenAI's application does not, as such, appear to be a concern for individual privacy or corporate data, provided that care is taken regarding the elements on which the robot is queried. What will happen to AI in other applications, even recreational ones, when deepfake scams have multiplied, or to commercial AI when user companies and consumers discover that personal data has been used to train the algorithm?

Consumer concerns, particularly in France and Europe, seem to make compliance with the GDPR and the AI Act a strong selling point. This is especially true when faced with competitors who may not have the same concerns about the lack of national rules on the matter, particularly in the United States, where the rules are more flexible and often left to the initiative of individual states.

Cited in a recent report by the Parliamentary Office for the Evaluation of Scientific and Technological Choices (OPECST), Bertrand Braunschweig, scientific coordinator of the confiance.ai program and former research coordinator of the national artificial intelligence program, confirms that the subject of trust in AI is *"a fundamental aspect for developers and public authorities alike, as well as an essential condition for the smooth and efficient deployment of technologies."*

HAVE MORE RELIABLE TOOLS AND DATA

In a 2018 survey, at the dawn of the GDPR, 55% of French consumers surveyed admitted to having already intentionally given incorrect personal information for

[116] PWC study, "Global Consumer Insights Survey", March 16, 2022.

[117] INSEE study, "82% of Internet users protect their personal data online", July 21, 2022.

fear that some of their information would be disclosed, usurped or stolen[118].

Shortly before, 90% of French people surveyed said they were in favor of the commercial use of their personal data in cases where they could express prior consent and have control over this data. It would therefore be more the conditions of data collection and use, rather than the use itself, that poses difficulties.

The various figures cited regarding fears due to the development of AI reinforce the idea that a framework can be beneficial both for the acceptability of the system itself and for the quality of the data that consumers are willing to integrate into it. When data is the fuel of these systems, the better and more reliable it is, the more coherent the system will be.

Also, the following benefits have been encountered for example for the GDPR[119]: better positioning in calls for tender, particularly public ones, but also in negotiations between professionals, better customer confidence, better targeting of communication, an improvement in certain business processes, a reduction in the mass of data processed with positive consequences in terms of CSR.

It's then up to companies to bridge the gap between law, communication, and marketing to maximize their benefits. Guides, labels, and certifications can then be a complementary asset.

2. From internal acceptability to the export of our standards

To validate the usefulness of a rule applied to innovation, the argument of acceptability therefore appears, initially, valid. It must also allow our companies to use their virtues, validated in part by law, in an international framework, in order to be able to conquer markets other than their own original market.

Thus, imposing rules on a market the size of the European Union[120] has two main interests:

- Force external actors to comply with it for their activities on this market,
- Consequently, impose our rules throughout the world, since it will be technically difficult to justify applying different rules depending on the markets and politically very complicated to present projects that offer less in terms of guarantees.

This is where national regulators and the European Commission have an immense responsibility. If they refuse to apply the rules that our national and European stakeholders adhere to, they will offer external stakeholders a major advantage and will permanently, if not permanently, weaken our model.

At the same time, another international player is eyeing this regulatory niche: China. As early as 2023, Democratic US Senator Chuck Schumer called on the United States to take the lead on regulation following China's presentation of its new approach to AI regulation in April 2023.

[118] Study conducted by YouGov Plc for RSA, carried out between 15 December 2017 and 3 January 2018.

[119] Results of a Wavestone study commissioned by the CNIL Digital Innovation Laboratory at the end of 2021 and published in May 2024

[120] In 2023, the European Union represented a gross domestic product (GDP) of 16,970 billion dollars against 27,720 billion for the United States and 17,790 billion for China.

Obviously, innovation must not be sacrificed on the altar of normative dogmatism. But in the absence of any dedicated standards, external markets will quickly be closed to innovators who have benefited from complete deregulation . In other words: whether any country likes it or not, an innovation will always be subject to rules sooner or later, whether it likes it or not.

In this scenario, there are only two possibilities: to close a certain number of external markets, or to conform to the rules of the game of the coveted markets in the hope of having gained sufficient technological and financial advance to be able to collect a significant compliance, if it is possible and the product has not been purely and simply banned.

With the risk, in the first case, of finding oneself in a highly vulnerable position given the extraterritoriality of external rules, as the United States was able to impose in the past with the extraterritoriality of its anti-corruption rules, allowing the acquisition of numerous large French and European companies placed at the mercy of enormous sanctions across the Atlantic.

ENSURE THE EXTRATERRITORIAL SCOPE OF DEDICATED LEGISLATION TO INNOVATIONS

The AI Act[121] and the GDPR[122] have this extraterritorial scope, since they apply whether the entity concerned is established in or outside the European Union. It is only the location where the services are offered, whether within the European Union or not, that will determine the application of the rule. With additional extraterritoriality for the GDPR in cases where data of individuals located in the European Union are used.[123]

Intellectual property law can also have this scope when it is rights determined from the location where the holder is located that are protected.

This is common sense and welcome because these rules then also radiate throughout the company's activity and can no longer be truly adjusted on a case-by-case basis, once the AI is trained with data that does not respect this principle.

Extraterritoriality is then less relevant when it comes to other cross-cutting legal governance rules (social law, competition law, intellectual property law) or sectoral rules (banking and financial law) that will apply to a given territory and operations without having consequences on the overall identity of an AI system. Not providing for extraterritorial effects in these cases therefore seems less serious at first glance.

This is in fact once again becoming a major issue with regard to sustainability rules, particularly the duty of care. Can these rules be supported without distorting competition to the disadvantage of national players if they only apply to these players ?[124] It is for this reason that a duty of care at the European level, with the

[121] Article 2, 1 of the AI Act.

[122] Article 3, 2 of the GDPR.

[123] Article 3, 2, b) of the GDPR.

[124] For another example: this is partly why French anti-corruption rules have extraterritorial scope since they apply to foreign companies above a certain threshold of employees and turnover. See Article 17, I of Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (known as the "Sapin 2 Law").

same requirements as the French duty of care, is essential. Because these are once again elements that go beyond the scope of a single territory or a single operation and must therefore apply to any company that undertakes to develop or use an AI system in the European Union, as soon as a French company of the same size would be concerned.

Part of the solution could be found in the European directive that plans to extend the European duty of care to companies, including those from third countries, as soon as part of their activities are carried out on the European market, from a certain turnover[125]. And in the CSRD directive, regarding information relating to sustainability, which provides for the same approach. This will both force large digital companies to impose sustainability rules in their value chain, and large external companies that will deploy these systems to call upon virtuous actors, who make the required data available.

C. THE RULE OF LAW AS A TOOL OF CONQUEST

The rule of law can become, for our companies, a tool for conquering markets, both public and private. When the United States regularly uses the extraterritoriality of certain national rules, particularly in the area of anti-corruption, to weaken foreign companies competing with national players, we also have the means to protect ourselves against foreign players who would play by rules other than those designed for respect our values.

The rule of law can then become, for our society, a tool for global conquest, given the challenges raised by AI. At this level, it is ultimately a matter of a meeting with history that public decision- makers, regulatory authorities, and courts must attend.

1. A market acquisition tool

The weapon of law, in a case of acquisition of markets, can be used by two levels:

- at the level of the regulator and the courts, through the rigorous application of existing legal frameworks.
- by national economic actors themselves, to obtain public or private contracts and before the courts, when they find themselves confronted with actors operating illegally, in the field of unfair competition.

THE RULE OF LAW AS A TOOL FOR THE ACQUISITION OF PUBLIC CONTRACTS

The rule of law is first and foremost a toll rule, in that it must allow those who violate it to be excluded. It can then be a rule that facilitates, as is the case with innovative public procurement. On this second point, the enabling framework has yet to be established.

Law as a toll rule. In terms of an actor's admissibility, GDPR compatibility can, for example, be a strength in obtaining public contracts when this contract

[125] Article 2, 2 of the European directive on the duty of vigilance.

involves personal data.

The subject was thus opened in 2021 by the Belgian Council of State[126], which accepted the request of a company that had not been selected in the call for tenders, although it considered that it complied with the GDPR unlike the selected competitor, in the context of a contract involving the processing of personal data, since it involved establishing a mobility center in order to facilitate the operation of public transport services.

Logically, calls for tender involving an AI solution must lead the public buyer to pay close attention to this subject, at the same time as to the guarantees implemented by the winning company, during the execution of the contract. Otherwise, an unsuccessful competitor could refer the matter to the administrative court and attempt to obtain the cancellation of the contract award in the event of insufficient verifications. The same logic will most certainly apply to compliance with the GDPR or the AI Act whenever the contract involves a use defined otherwise than by minimal risk.

Thus, the European Commission and national CNILs are carrying out significant work to regulate AI. Meta, for example, had to curb its ambitions to train LLMs with content found on the group's social networks. This work must help public actors to be equally vigilant.

To this end, public actors must equip themselves with the necessary legal tools and therefore pay close attention to the specific clauses of the contract. The General Administrative Clauses Books (CCAG), which provide for the conditions of execution applicable to categories of public contracts, have already been updated in this regard since 2021.

But it is up to each public buyer to provide both adequate and sufficient clauses regarding innovations and the applicable penalties; even general principles could be invoked where appropriate, which could also include the sustainability rules provided for by law[127].

On this subject, the Public Procurement Code offers an exemption procedure for innovative procurement, in order to encourage public procurement from smaller companies. However, the mechanism remains underutilized. This is particularly true because this procedure is still poorly understood by stakeholders, who see it as an additional risk area.

The idea could be to simplify the normal procedure, and AI can be a valuable aid in this case. This is an example of what the startup Explain is promoting, using it to respond as efficiently as possible to public procurement.

[126] Belgian Council of State, 12 May 2021, no. 250.599. This case law is supplemented by two other decisions of the Belgian Council of State: CE, 23 December 2019, no. 246.532 and CE, 6 May 2022, no. 253.677.

[127] Article L2152-1 of the Public Procurement Code thus requires the public buyer to reject irregular, unacceptable or inappropriate offers. Article L2152-2 describes as irregular *"an offer which does not comply with the requirements set out in the consultation documents, in particular because it is incomplete, or which disregards the applicable legislation, particularly in social and environmental matters."*

THE RULE OF LAW AS A TOOL FOR ACQUIRING PRIVATE CONTRACTS

This compatibility of innovation with French and European law should also be a strength for start-ups wishing to integrate their technical solutions with other economic players. It limits the risk of litigation for the co-contractor, who would then be held responsible for the lack of conformity, and makes it possible to offer a solution that, by nature, will be more acceptable to the end consumer.

In this private law framework, the GDPR is, finally, a weapon that can be seized companies in compliance to protect themselves from unscrupulous actors.

The Paris Judicial Court and the Paris Court of Appeal have ruled in the last two years that unfair competition consists of "*actions that deviate from the general rules of loyalty and professional probity applicable in economic activities and governing business life, such as those creating a risk of confusion with the products or services offered by another operator*"[128], thus implying non- compliance with the GDPR[129]. In the present cases, the breaches noted concerned in particular the absence of a charter and consents collected in conditions contrary to the required requirements.

This practice was recently confirmed by the Court of Justice of the European Union, questioned on the compliance of such sanctions with the GDPR[130]. Here again, it seems serious to consider that the same reasoning could apply to the AI Act, each time the use requires special attention, that is to say for all use cases other than those classified as minimal risk.

Similarly, as noted previously, the participation of AI providers in the necessary feedback regarding duty of care is an additional compliance opportunity for the players subject to it, and as such should be taken as an asset by the latter.

The interest in these cases of use of law as an economic weapon must obviously be reinforced by the case law of the courts and decisions of the national CNILs and the European Commission, particularly with regard to the guarantees of conformity expected from actors outside the European Union concerning the protection and use of personal data.

At this point, the two levels of use of the weapon overlap since the responsibility of the courts and the regulator in the cases submitted to it depends on the degree of commercial offensiveness that the private actor will have in the face of competitors who show little respect for the rules of law.

[128] See in particular: Paris Judicial Court, April 15, 2022, no. 19/12628 and Paris Court of Appeal, November 9, 2022, no.21/00180.

[129] The Commercial Chamber of the Court of Cassation had already ruled that "Failure to comply with regulations in the exercise of a commercial activity, which necessarily results in an unfair competitive advantage for the perpetrator, constitutes an act of unfair competition." Cass. Com., March 17, 2021, No. 01-10.414.

[130] CJEU, 4 October 2024, ND v DR, case C-21/23

2. The meeting with the history of political decision-makers, regulatory authorities and jurisdictions

Artificial intelligence is driving a profound upheaval in our economies and societies. France and the European Union as a whole are at a decisive moment. Each of our choices—economic, legal, and political—is likely to determine the role we will play in the world for many years to come.

However, at this time of decision, we still have the means to bring, even onto the world stage, an ethical, sustainable and competitive AI as a flagship of our sovereignty.

To achieve this, the law must become a proud weapon. We must abandon the impression of having the law ashamed of those who think they are too big to comply with it, and apply it (too) firmly only to our national and European actors who are the first to play the game, even if forced.

THE HISTORICAL ROLE OF PUBLIC DECISION-MAKERS

In this meeting with history, public decision-makers must bear a clear vision of the law.

In recent years, rules have accumulated. This is a fact and not necessarily a bad thing, provided that stakeholders are supported to comply with them, with the necessary time and flexibility. This permanent regulation may be a strategy, but in this case it seems perilous given the resources available to our national and European stakeholders in the face of foreign giants, often fueled by state funds.

We offer:

- **Limit any new rules dedicated to digital technology, and in particular to AI, to rules that aim to simplify existing rules to make them more accessible ,** to standardize interpretations between European countries, to coordinate regulations, and to strengthen European sovereignty and strategic autonomy.
- **Retain an adapted vision of the law with the three layers inspired by information-matic: infrastructure, platform and service.**
- Regardless of the scenario chosen, a clear vision is necessary. So that stakeholders know in which direction they should move forward. This same vision should normally prevail when it comes to tax rules. **In law, the first security is predictability.**

THE HISTORICAL ROLE OF REGULATORY AUTHORITIES

In line with the logic of digital texts, particularly the GDPR, the risk-based approach should constitute an unalterable key to understanding. To achieve this, each case should be analyzed in great detail based on the specificities of the sector and the technology used, and sanctions should be established, where appropriate, based on all of these elements.

The CNIL, with regard to data, strives to provide answers on these subjects but

sometimes finds itself confronted with the difficulty of specific cases and media pressure amplified by social networks, in a few emblematic cases.

To limit these risks which weaken the legitimacy of the structure as a whole, it could be envisaged (i) to intensify the logic of proactive and agile regulation with a permanent dialogue with innovative ecosystems, and (ii) to better represent the actors of new technologies in the college of the CNIL.

On this last point, parliamentary work is underway and moving in this direction, this must be emphasized. While no system is perfect, the presence of a greater number of professionals from the sector seems useful to intensify the dialogue with the lawyers who do a very important job, which will be even more valued when it gains full legitimacy from exchanges with the stakeholders.

The establishment of a national network for coordinating the regulation of services digital[131] by the SREN law also goes in this direction, of a better knowledge of sectoral specificities and must be supported until the end.

These reflections are far from trivial. Because without regulation that is understood by all, that is, perceived as fair, we will not be able to make the law the weapon it can and should be.

The responsibility of the regulatory authorities is immense in this regard.

THE HISTORICAL ROLE OF THE JURISDICTIONS

Finally, the courts, as an extension of the regulatory authorities and in their role as guarantors of fundamental balances, must be up to date with the realities of artificial intelligence and, more broadly, digital technology.

They play an essential role in the interpretation of new standards, which can sometimes miss their target or require very careful reading, including the context and technical realities.

[131] Composed of all the competent administrative authorities and the main State services, including the General Directorate for Competition, Consumer Affairs and Fraud Control (DGCCRF) and the General Directorate for Enterprise (DGE), this network, led by the DGE, will be responsible for strengthening multilateral cooperation in order to enable better coordination of digital regulations between them.

AI WITHOUT RULES
IS POWER WITHOUT
CONSCIENCE.

CONCLUSION

"Our choice is not between "regulation" and "no regulation". (...) The only choice is whether we collectively will have a role in (coders) choice and thus in determining how these values regulate or whether collectively we will allow the coders to select our values for us"[132]

Lawrence Lessig

Twenty-five years after Professor Lessig's analysis, AI is a formidable pretext for re-examining the relationship between law and digital technology. On the one hand, because its potential and the need to be at the forefront in order to hope to exist, largely call into question the legal framework that, in Europe at least, had allowed the transition from "Code is Law" to "Law is Code." On the other hand, because AI carries within itself the characteristics of a technology capable of reinventing the relationship between law and innovation, for the better.

With this report, we have therefore tried to answer, in our own words, this question: **to succeed in developing and imposing European AI, must we choose between innovation and regulation?**

Our conviction is simple: if we want to preserve a world for all, the two go hand in hand. Innovation has no meaning or collective impact without strict, clear, and strategic regulation.

These are the conditions for an alliance of these two false opposites that we have therefore attempted to identify, for the case of artificial intelligence.

These conditions are three in number:

- The standard must facilitate scalability,

- The standard must accelerate its acceptability,

- The standard must be activatable to become a lever for market acquisition.

The rule of law can thus give innovation direction and value. **The report proposes a political and strategic architecture to achieve this while fully in line with the reflections of Enrico Letta and Mario Draghi** on the need to strengthen European integration to face contemporary economic and technological challenges.

Where Letta proposes a 28th regime to facilitate access to law and Draghi calls for a deep consolidation of the European internal market, *AI is Law* asserts that coded and intelligible law will be one of the key tools to make this ambition operational in the era of artificial intelligence.

[132] L. Lessig, "Code and other laws of cyberspace", Basic Books, 1999.

Because the self-appointed apostles of freedom are sometimes its greatest enemies. In a world where AI will soon be the author of the code, leaving the choice of our values to coders would be letting down much more than our values: it would be letting down humanity.

RECOMMENDATIONS

ADAPT THE ARCHITECTURE OF LAW TO THE NEEDS OF AI

Why? The law must become a lever for scaling innovation: it protects, legitimizes, and secures innovation.

What? The architecture of the law must be adapted to accommodate technologies that evolve faster than the norm, without losing its protective logic for society. An architecture inspired by computer science can be proposed:

- ***Law as an Infrastructure (LaaI):*** with freedoms and rights unalterable fundamentals guaranteed by nature.
- ***Law as a Platform (LaaP):*** codable legal texts (an "API right"), starting with the data-related texts.
- ***Law as a Service (LaaS):*** an experimental scope within a flexible but secure framework, based on the model of regulatory "sandboxes".

How?

- **Recommendation No 1** | Make code the 25th language of the European Union so that any new text can be translated into computer language.
- **Recommendation No 2** | Integrate a coding text of the right to omnibuses in preparation at European level of modifications to allow the short-term coding of the main texts dedicated to digital, in line with the work already started.
- **Recommendation No 3** | Initially, promote the Legal Data Space initiative at the French level, which already brings together a large number of players in the legal sector. This is a shared infrastructure for processing and sharing public legal data - open data - and private data - data spaces - with the aim of developing a sovereign legal AI, by and for the legal sector.

PROMOTE A READABLE, HARMONIZED AND SOVEREIGN

Why? To be a lever for innovation, the rule of law must be predictable, intelligible, and actionable.

What? Adjust the existing set to bring greater coherence and strategic ambition.

How?

- **Recommendation No 4** | Simplify, harmonize, articulate and to sovereignize by limiting the next modifications of the legal framework to these objectives.

- **Recommendation No 5** | Evaluate the effectiveness of rules dedicated to AI based on the triptych: standardization (the rule must be a lever for scaling innovation), acceptability (the rule must facilitate the acceptability of innovation), actionability (the rule must allow stakeholders to take advantage of it in conquering markets).

SIMON BERNARD

Simon Bernard is a lawyer, founder of the law firm ModernLaw, dedicated to governance and the challenges of artificial intelligence.

Simon began his career in international taxation and actively contributed to work on the taxation of digital giants and to the first writings on the taxation of the blockchain ecosystem. Following this, he joined the majority group in the National Assembly, advising first on matters of taxation and public finance, then on sovereign and civil liberties issues, notably the laws of the Ministries of the Interior and Justice, and all texts relating to the health crisis.

He then joined the office of a Prime Minister as a parliamentary advisor, contributing to the preparation, negotiation, and monitoring of texts relating to the Ministries of the Interior and Justice, local authorities, overseas territories, issues related to energy and ecological transition, and digital regulation, in particular. He subsequently became Deputy Director of the Minister of Sports and the Olympic and Paralympic Games, in charge of ethics and integrity.

In March 2025, he founded the law firm ModernLaw, dedicated to governance and the challenges of artificial intelligence, in order to support both tech players and all public and private stakeholders in this new environment. In this context and in line with his career and the philosophy of the “AI is Law” report, Simon defends a vision of law as an economic and strategic lever, a tool of sovereignty and an accelerator of transitions that benefit everyone.

THANKS

This report would not have been possible without the support and expertise of several individuals and organizations whose commitment and vision were instrumental in outlining the conditions and contours of a law that would both shield and spearhead an ambitious and responsible European AI.

I would like to express my deepest gratitude to the think tank, and in particular to Arno Pons and Olivier Dion. Their trust, their valuable guidance, and their consistently constructive advice have helped us find relevant and very concrete avenues.

My thanks also go to Martin Bussy and Thomas Saint-Aubin, pioneers in the perception of law as a lever for scalability. Their work on the Legal Data Space already constitutes an essential infrastructure foundation, ahead of the legal architecture proposed in this report.

I would like to warmly thank all the stakeholders, public decision-makers , and advisors who kindly shared their experience of law as it relates to innovation and the development of artificial intelligence with us, particularly Criteo, Explain, France Digitale, and Numeum. Your experiences and ideas were extremely valuable and contributed to the depth of the analyses presented.

Finally, special recognition goes to Clara Koenig and François. For their wise advice, their infectious passion for these complex subjects, and their keen insight that enriched this report at key moments.

To all, a big thank you. This report is now ours, the report of those who believe to the values and strength of our dear and today so precious democracy.

DIGITAL NEW DEAL
THINK-DO-TANK OF THE NEW DEAL

Digital New Deal supports private and public decision-makers in creating a European and Humanist Digital Enlightenment. Our belief is that we can offer a third digital way by pursuing a dual objective: defending our values by proposing a framework of trust through regulation (think tank); and defending our interests by creating ecosystems of trust through cooperation (do tank).

Our publishing activity aims to shed as much light as possible on the developments taking place within the issues of "digital sovereignty", in the broadest sense of the term, and to develop concrete courses of action for economic and political organizations.

Olivier Sichel (founding president) and Arno Pons (general delegate) steer the strategic directions of the think-tank under the regular supervision of the board of directors (composition below).

SÉBASTIEN BAZIN
CEO of AccorHotels

NATHALIE COLLIN
General Manager, Consumer and Digital Division La Poste Group

NICOLAS DUFOURCQ
DG of Bpifrance

AXELLE LEMAIRE
Former Secretary of State for Digital Technology and Innovation

ALAIN MINC
President of AM Conseil

DENIS OLIVENNES
DG Libération

ODILE GAUTHIER
DG of the Institut Mines-Telecom

ARNO PONS
General Delegate of the Digital New Deal think tank

BRUNO SPORTISSE
CEO of Inria

ROBERT ZARADER
CEO of Bona Fidé

JUDITH ROCHFELD
Associate Professor of Law, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
Deputy Director General of the Caisse des Dépôts

OUR PUBLICATIONS

Generative AI: unite or submit
Olivier Dion, Michel-Marie Maudet, Arno Pons – *November 2024*

Public data sharing infrastructures: the great forgotten
Laura Létourneau – *September 2024*

Strengthening pan-european democracy in the era of AI
Axel Dauchez, Hendrik Nahar – *April 2024*

Digital technology for a sustainable future
Véronique Blum, Maxime Mathon – *June 2023*

Trusted AI, a strategic opportunity for industrial and digital sovereignty
Julien Chiaroni, Arno Pons – *June 2022*

Trusted data, data sharing, the key to our strategic autonomy
Olivier Dion, Arno Pons – *September 2022*

Cybersecurity, the guardian of our strategic autonomy
Arnaud Martin, Didier Gras – *June 2022*

GDPR, Act II: Collective control of our data as an imperative
Julia Roussoulières, Jean Rérolle – *May 2022*

Digital taxation, the return match
Vincent Renoux – *September 2021*

Defending the rule of law in the age of platforms
Denis Olivennes et Gilles Le Chatelier – *June 2021*

Trusted Cloud: A Strategic Autonomy Issue for Europe
Laurence Houdeville et Arno Pons – *May 2021*

White papers: Data sharing & tourism
Fabernovel et Digital New Deal – *April 2021*

Sharing personal data: changing the game through governance
Matthias de Bièvre et Olivier Dion – *September 2020*

Reflections on the European Digital Services Act
Liza Bellulo – *March 2020*

Preserving our educational sovereignty: supporting French EdTech
Marie-Christine Levet – *November 2019*

Breaking the Big Tech Monopoly: Regulate to Free the Many
Sébastien Soriano – *September 2019*

Getting out of digital Stockholm syndrome
Jean-Romain Lhomme – *October 2018*

The Citizen Public Service
Paul Duan – *June 2018*

The Age of the Decentralized Web
Clément Jeanneau – *April 2018*

Real taxation for a virtual world
Vincent Renoux – *September 2017*

Regulating "digital"
Joëlle Toledano – *May 2017*

Call to presidential election candidates for a #DigitalPact
January 2017

Health in the face of the tsunami of NBICs and platformers
Laurent Alexandre – *June 2016*

What is the personal data policy?
Judith Rochfeld – *September 2015*

State of digital technology in Europe
Olivier Sichel – *July 2015*

THINK-DO-TANK

DIGITAL NEW DEAL

June 2025

www.thedigitalnewdeal.org