UCLouvain

LOUVAIN
School of Management

Louvain School of Management

Navigating the Intersection of the DMA and GDPR: Impacts on data-driven Markets in the EU

Author(s): Quentin Roland
Supervisor(s): Bernard Paque
Academic year 2024-2025
Dissertation for the Master [120] in Management with a focus in European Business
Daytime schedule

Declaration on the Use of AI Tools in the Master's Thesis

During the preparation of this master's thesis, I made use of several artificial intelligence tools in a responsible and transparent manner, in accordance with academic integrity standards. The following tools were used:

1. ChatGPT (OpenAI):

ChatGPT was used to support the formulation of arguments, identify structure improvements, and refine academic phrasing. It also served as a brainstorming assistant for highlighting key trade-offs between GDPR and DMA. All content generated with this tool was critically reviewed, edited, and adapted by myself.

2. DeepL (Pro and Write): There were two key reasons why DeepL was used:

Translation: To translate parts of the thesis or source documents from French to English and back again more accurately and quickly.

DeepL Write was utilized to enhance grammar, coherence, and clarity in English. All recommendations were looked over and changed to make sure they fit with the goals of the thesis and the author's style.

3. TurboScribe: We utilized TurboScribe to write down what people said in audio recordings of interviews. This program made it possible to transcribe spoken content more quickly, and then it was manually adjusted and anonymised when needed. I checked the meanings and quotes that came from these interviews.

After using these tools, I carefully looked over, fixed, and checked all of the content that came out of them. I am fully responsible for the final content of this thesis.

I agree that the content of my master's thesis is my own original work, with the help of artificial intelligence tools that I used in a responsible and open way.

Done in Brussels on the 15th of July 2025,

Quentin Roland

Acknowledgements

I would like to express my sincere gratitude to Mr. Bernard Paque, my thesis supervisor, for his invaluable guidance throughout this research. His expertise, availability, and thoughtful feedback greatly enriched my work. I am especially thankful for his methodological rigor, critical perspective, and the many stimulating ideas he helped me explore.

I would also like to warmly thank all the individuals who agreed to participate in my interviews. Their insights, experience, and willingness to share their knowledge provided essential depth to this thesis.

I want to thank my family and friends from the bottom of my heart for always being there for me during this difficult time. Their support and understanding helped me keep on track and motivated.

Finally, I would like to thank all future readers of this thesis. I sincerely hope that it will prove insightful and thought-provoking.

Abstract

This thesis explores the evolving interaction between two cornerstone EU regulations: the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA), and their combined impact on digital business models and innovation within the European Union. Adopting a qualitative and exploratory methodology, the research is based on expert interviews with regulators, legal scholars, startup founders, and corporate professionals. It analyses how European firms adapt to these regulations depending on their strategic posture as regulatory takers or shapers, and evaluates the trade-offs experienced by various stakeholders including large platforms, SMEs, consumers, and policymakers.

The results show that the GDPR's focus on privacy and the DMA's focus on market fairness and contestability can work together and against each other. Each rule encourages user empowerment and competitive dynamics on their own, but when they are put into effect together, they still have problems with enforcement that isn't consistent and governance that isn't connected. Case studies show how these rules hinder the ability to innovate, especially for European companies trying to compete with non-EU IT giants.
In the end, this study raises the question of whether the existing regulatory framework really makes things better for consumers and gives European digital markets a long-term competitive edge.

Table of content

1.Introduction

Over the past decade, digital platforms have fundamentally reshaped the European economy. From social media to e-commerce and cloud infrastructure, digital services have become essential to the way companies operate, citizens communicate, and governments function. However, this growing dependence on digital technologies has also brought new challenges. A handful of large technology firms, commonly referred to as "gatekeepers", have come to dominate online markets, controlling not only access to digital infrastructures but also the flow of personal data. Their power raises concerns regarding market fairness, consumer protection, and democratic accountability.

In parallel, personal data has emerged as one of the most strategic resources of the digital era. Business models based on behavioral profiling, targeted advertising, and algorithmic decision-making have intensified the need to collect, process, and monetize user data at an unprecedented scale. These practices, while highly profitable, have triggered debates about privacy, data sovereignty, and the ethical use of information. In response to these developments, the European Union has enacted a series of landmark regulations aimed at fostering a fairer and more transparent digital environment.

Two of the most emblematic texts are the General Data Protection Regulation (GDPR), which came into force in 2018, and the Digital Markets Act (DMA), adopted in 2022. While the GDPR focuses on reinforcing individual rights and strengthening data governance, the DMA targets structural imbalances in digital markets by introducing obligations for dominant platforms. Each of these regulations addresses different challenges, yet they overlap in scope, especially in areas such as data sharing, interoperability, and algorithmic transparency. This convergence creates both synergies and tensions, particularly for firms that must adapt their business models to remain compliant while staying innovative and competitive.

In light of these regulatory developments and their growing impact on digital actors, an essential question arises: **To what extent does the interaction between the Digital**

Markets Act and the General Data Protection Regulation influence the business models and innovation strategies of European firms operating in digital markets?
This question is especially relevant in the current context, where European regulators are asserting a more proactive role in shaping the global digital economy, while firms increasingly operate across jurisdictions with diverging legal requirements. By examining how the GDPR and DMA influence corporate strategy, innovation capacity, and compliance mechanisms, this research seeks to shed light on the broader transformation of digital capitalism in Europe.

The choice of this topic also stems from professional exposure to the dynamics of platform regulation during my final-year internship, as well as a broader interest in the intersection between law, technology, and business strategy. Although the initial research design included a larger number of expert interviews, several potential participants declined to take part, which somewhat limited the empirical base. Nonetheless, the interviews conducted provided valuable insights into the operational and strategic impact of these regulations. These were complemented by academic literature, policy reports, and official documents from European institutions.

To answer this question, the thesis is structured into four chapters, each addressing a key analytical dimension. Chapter 1 offers a literature review introducing the evolution of digital markets, the rise of platform dominance, the economic role of personal data, and the emergence of the GDPR and DMA. Chapter 2 analyses the technological and economic foundations of data-driven platforms, as well as the risks associated with unregulated digital markets. Chapter 3 investigates how firms experience and respond to regulatory requirements, using case studies to illustrate adaptation strategies and trade-offs. Chapter 4 discusses the broader implications of the European approach, weighing its advantages and limitations in a globalized context, and identifying future perspectives.

By analysing the intersection of the GDPR and DMA, this research contributes to the academic and policy debate on how best to reconcile innovation, competition, and fundamental rights in an increasingly digitalized world.

2. Literature review

2.1. Context of Digital Markets

2.1.1. The increasing significance of technological platforms

Over the past fifteen years, technological platforms have emerged as the dominant infrastructure of the European digital economy. Companies such as Apple, Amazon, Google, Meta, and Microsoft often referred to collectively as GAFAM have played a central role in reshaping how markets operate by controlling access to core services like search engines, ecommerce, operating systems, social media, and cloud computing. These firms do more than participate in markets; they increasingly define them (see Figure B.1.). Their dominance stems from a combination of multi sided market dynamics, powerful network effects, and strategic vertical integration, making them incredibly resilient to disruption and difficult to challenge using traditional business models (Crémer, de Montjoye & Schweitzer, 2019).

A good example of this dominance is the European digital advertising market, which was worth over €85 billion in 2022. Google and Meta alone captured more than 70% of that value, with Amazon quickly gaining ground thanks to its use of retail data to strengthen its ad offering (European Commission, 2023). In the mobile space, Apple's iOS and Google's Android together controlled 99.6% of the EU operating system market in 2023. This kind of control effectively forms a duopoly and allows them to set the rules for third party developers, including charging commissions of up to 30% on in app purchases (Statista, 2023).

What sets these platforms apart is their role as gatekeepers. According to the Digital Markets Act (DMA), a gatekeeper is a company that stands between businesses and consumers, shaping how they interact and benefiting from a position of entrenched and lasting power (European Commission, 2022). For example, Amazon can prioritize its own products in search results, Apple can restrict alternative payment systems on its devices, and Google can give preference to its own services practices. These practices have been the subject of multiple antitrust investigations in the EU.

These firms also benefit from significant economies of scale and data network effects. The more people use a platform, the more data it collects, and the better it becomes at delivering personalized services, advertising, and user experiences. For instance, Google processes over 8.5 billion searches a day. Every one of those searches helps refine its algorithms, creating a competitive edge that is extremely difficult for newcomers to match (Wang, Zhang & Wang, 2021).

Moreover, these platforms are now central players in the development of artificial intelligence (AI). The five leading global cloud providers AWS, Microsoft Azure, Google Cloud, Alibaba Cloud, and IBM host most of the world's AI training processes (OECD, 2023). This not only gives them control over the infrastructure that powers AI but also places them in a position to shape the future of digital innovation. Many European firms willing to build AI based tools must rely on these same providers, creating long term dependencies that raise concerns about their technological sovereignty.

To strengthen their grip on the market, dominant platforms often engage in platform envelopment a strategy of expantion into related markets to absorb more user data and reduce the likelihood that users will switch to alternatives. For example, Meta acquired Instagram and WhatsApp to consolidate its control over social communication, while Amazon moved from retail into logistics, cloud computing, and media (Evangelista, Guerrieri & Meliciani, 2014). This makes it harder for regulators to even define what market a platform operates in, let alone intervene effectively.

Still, some European alternatives have attempted to chart a different course. Companies like Qwant (search), Nextcloud (cloud storage), Mistral (IA) and Brave (browser) have positioned themselves as privacy focused or open source options. However, their market share remains marginal, and their growth is limited by scale, visibility, and funding challenges (BEUC, 2022).

From a business perspective, platforms offer clear benefits. They reduce transaction costs, connect supply and demand efficiently, and open up new ways of creating value through targeted marketing**,** dynamic pricing, and user driven innovation. But they also create lock

in effects and new kinds of dependency. In many cases, companies can no longer afford not to use these platforms. If they do not, they risk losing visibility, customers, and revenue.

The rise of platforms has also transformed traditional industries. In mobility (Uber), accommodation (Airbnb, Booking), food delivery (Deliveroo), and freelance work (Fiverr), platforms have shifted the focus from physical assets to digital interfaces and data flows. Control over users, not factories or warehouses, is now the key source of power (OECD, 2019).

Finally, while dominant platforms continue to concentrate market power, the academic literature suggests that not all technological development is structurally locked into these ecosystems. As De Propris and Corradini (2013) emphasize, technology platforms, particularly those supported by key enabling and bridging technologies, can foster cross-sectoral innovation and contribute to the emergence of more original forms of value creation. This indicates that even in markets marked by strong concentration, there is still room for European firms to innovate independently, provided that the institutional and regulatory environment supports such dynamics. In this light, the Digital Markets Act represents a structural response to platform dominance, introducing proactive obligations for gatekeepers with the aim of restoring contestability, preserving user choice, and strengthening the European Union's capacity to shape its own digital trajectory.

2.1.2. The Impact of Personal Data in the Digital Economy

The role of personal data in the digital economy has become central to the way markets operate in Europe. Concerns about privacy**,** data protection, and power asymmetries have shaped both regulatory strategies and corporate behaviors. The transformation of personal data into an economic asset has changed how companies engage with consumers, optimize business models, and create value from digital interactions. For many firms, personal data is no longer a byproduct but a core driver of monetization strategies, supporting hyper personalized services**,** predictive analytics, and targeted

advertising that generate billions in revenue each year (Wang, Zhang & Wang, 2021, see Figure B.2.).

A defining feature of personal data is its centrality to algorithmic decision making and artificial intelligence. Major platforms like Google, Facebook, and Amazon rely on large scale data aggregation to refine recommendation engines, personalize content, and optimize pricing strategies. Through the use of big data analytics, these companies develop detailed user profiles based on behavioral patterns, preferences, and online interactions, enabling highly accurate and profitable forms of user targeting (Grundmann & Hacker, 2017). This process lies at the heart of programmatic advertising, where real time bidding systems determine which ads users will see depending on their digital activity.

To support these mechanisms, companies embed tracking technologies across websites, apps, and loyalty programs. This pervasive data collection often takes place without full consumer awareness, raising questions about autonomy and informed consent (OECD, 2019). The practice has created widespread dependency on data driven business models, where consumers trade personal data for access to free services, often without clear knowledge and understanding the extent or value of the information they provide.

The economic value of personal data is also enhanced by data network effects. The more a platform collects, the better its predictive tools and services become. This creates a feedback loop that reinforces competitive advantage and makes it harder for new entrants to challenge incumbents (Evangelista, Guerrieri & Meliciani, 2014). Search engines like Google benefit from millions of daily interactions to fine tune their algorithms. Similarly, ecommerce firms like Amazon optimize logistics and pricing based on constant streams of consumer data. These advantages contribute to market concentration, as firms with more data can outmaneuver competitors even if the latter offer more innovative products (Evans, 2018). As shown in the table (see Figure B.3.), online advertising revenues began to surpass traditional media well before regulatory intervention. This shift created both economic opportunities for platforms and structural risks related to data exploitation and market concentration.

These dynamics have also prompted deeper societal reflections on how data is collected and used. The concept of surveillance capitalism (Zuboff, 2019) highlights how companies extract economic value from users by converting digital behavior into monetizable assets. This raises ethical concerns about manipulation, nudging, and even political interference. The Cambridge Analytica case revealed how platforms could be used to influence voter behavior through micro targeting, sparking debates on the social risks of unchecked data use (Wang, Zhang & Wang, 2021).

To address these issues, the EU adopted the General Data Protection Regulation (GDPR) in 2018. GDPR created a legal foundation for data protection based on consent**,** data portability, and the right to be forgotten, forcing companies to adapt their practices (OECD, 2019). While large firms adjusted with relative ease, many small and medium enterprises (SMEs) have struggled to comply due to limited resources. As a result, GDPR has unintentionally and paradoxically reinforced the position of dominant platforms who can afford robust compliance systems (Evans & Schmalensee, 2017).

Beyond compliance, new models of data ownership have emerged in academic and policy debates. Some propose data dividends, where users would be compensated for the data, they generate (Evens, 2018). Others promote data cooperatives, where individuals pool and negotiate access to their data collectively. These models challenge the current system, but their viability remains uncertain due to legal, economic, and technical constraints.

Additionally, data governance has implications for international trade and digital sovereignty. Many governments now promote data localization policies to ensure that data stays within national borders. While these measures aim to enhance privacy and security, they risk fragmenting the global digital economy and increasing costs for businesses operating across multiple jurisdictions (Grundmann & Hacker, 2017). Firms must navigate a complex patchwork of rules including GDPR, US legislation, and emerging laws in China and other regions (OECD, 2019).

In short, personal data has become a cornerstone of the digital economy, shaping market structures, regulatory debates, and innovation trajectories. As businesses seek to extract

maximum value from user data, policymakers must strike a balance between promoting innovation and protecting rights. Emerging technologies such as privacy enhancing technologies, blockchain based identity tools, and decentralized data governance systems offer new possibilities. But ultimately, the future of digital markets will depend on how society defines ownership, accountability, and fairness in the age of data driven capitalism.

2.1.3. Market challenges before DMA and GDPR

Before the introduction of the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR), digital markets in Europe developed in a fragmented and weakly regulated environment. This lack of coordination allowed dominant technology platforms such as Google, Amazon, Meta, Apple, and Microsoft to consolidate their power through practices like platform envelopment, self-preferencing, and strategic mergers and acquisitions (Evangelista, Guerrieri & Meliciani, 2014; Evans & Schmalensee, 2017). These firms leveraged network effects, data-driven economies of scale, and algorithmic decision-making to outcompete rivals while avoiding clear antitrust oversight.

A major concern during this period was the opaque use of personal data. In the absence of harmonized privacy rules, platforms engaged in extensive behavioral profiling and tracking, often without informed user consent (Wang, Zhang & Wang, 2021). Scandals like Cambridge Analytica exposed how unregulated data flows could be exploited for political or commercial gain (Grundmann & Hacker, 2017).

Furthermore, fragmented national regulations across the EU enabled regulatory arbitrage, while the dominance of non-European platforms raised strategic concerns around data sovereignty and European technological autonomy (OECD, 2019). Platforms were often seen as neutral intermediaries, escaping accountability for misinformation, market distortions, and content moderation failures.

These accumulated issues exposed the limits of traditional regulatory tools and stirred pressure for a new legal architecture. The adoption of the DMA and GDPR responded to

these gaps by redefining rules on market fairness, data governance, and consumer rights, laying the foundation for a more resilient and sovereign European digital economy (Evans & Schmalensee, 2017).

2.2. Digital Market Act (DMA)

2.2.1. Combating the abuse of dominant positions by Gatekeepers

The Digital Markets Act (DMA), adopted by the European Union in 2022, was designed to address a growing concern: the excessive concentration of power in the hands of a few gatekeepers who no longer merely participate in digital markets but shape and govern them. These platforms provide essential core services such as search engines**,** app stores**,** cloud infrastructure**,** or operating systems and act as unavoidable intermediaries between businesses and users. This privileged position allows them to define the rules of access, influence visibility, and dictate the terms of competition, often without meaningful oversight (Ibáñez Colomo, 2021; Danois, 2024). In this environment, traditional competition law, especially Article 102 TFEU, appeared too slow, too fragmented, and too reactive to deal with systemic forms of exclusion.

The DMA introduces a structural shift. Rather than reacting to individual abuses, it sets out ex ante obligations that apply automatically to companies meeting the criteria of a gatekeeper**.** These obligations are designed to prevent behavioural patterns that are seen as inherently harmful to contestability, meaning the ability of a market to remain open to new competitors. Practices like self preferencing, the use of non public data from business users, or the restriction of access to device functionalities are no longer assessed case by case. They are simply prohibited, based on the assumption that when exercised by a gatekeeper, they reduce the possibility for others to compete on merit (Akman, 2021; Frison Roche and Roda, 2022).

A particularly contested example is self preferencing, where a platform ranks its own products or services more favourably than those of competitors. This behaviour, central to the Google Shopping case, was shown to distort user choices and limit visibility for rivals. Similarly, forcing users to keep preinstalled applications, denying access to APIs

(Application Programming Interface), or tying different services together are strategies that, while subtle, effectively close off markets (Crémer et al., 2019). By prohibiting these tactics, the DMA seeks not to punish size or success but to dismantle the mechanisms that make such success permanent and unchallengeable.

This approach reflects a broader understanding of how power operates in the digital economy. Dominance is not only about price or scale but also about architecture, friction, and information control. Gatekeepers design the systems through which consumers search, select, and engage. As such, they can shape markets to their advantage without appearing to do so. In response, the DMA imposes strict obligations intended to neutralise this silent power. It represents a form of asymmetric regulation, where only the most powerful actors are targeted with structural constraints in order to restore a fairer environment (Larouche and de Streel, 2021; Petropoulos et al., 2021). As Renda (2022) explains, the objective is to regulate not just behaviour but the infrastructural conditions under which competition occurs.

However, early implementation has raised doubts about how effective these obligations truly are in practice. For instance, recent user experiences with Meta illustrate persistent asymmetries. The rollout of new artificial intelligence features in WhatsApp has made it difficult, if not impossible, for users to deactivate or manage the functionality. Account settings across Meta services remain fragmented and attempts to exercise user autonomy often lead to opaque processes and unclear outcomes. These examples suggest that while the DMA formally requires choice**,** interoperability**,** and data separation, its practical enforcement may lag behind technical reality. Such concerns are also reflected in Valletti and Zingales (2021), who argue that the capacity of dominant firms to circumvent regulatory intentions through design choices remains underestimated by policymakers.

This gap between regulatory ambition and user experience raises a fundamental question. Can the DMA truly rebalance power in digital ecosystems, or will it become a symbolic framework whose impact remains mostly legalistic? According to The Art to Make Gatekeeper Positions Contestable (2022), meaningful contestability requires more than legal rules it demands monitoring infrastructures, enforcement capabilities, and

institutional coordination at scale. Answering this therefore requires more than legal texts. It calls for continuous scrutiny, technical audits, and political resolve to confront the evolving strategies of powerful actors. Only under these conditions can the DMA succeed not just in rewriting the legal rules of the digital economy but in reshaping how that economy actually works.

2.2.2. Enhancing Interoperability and Market Fairness

A second major goal of the Digital Markets Act (DMA) is to promote interoperability and fairness in digital markets. These principles are key to addressing the structural asymmetries that allow certain gatekeepers to dominate ecosystems. Defined in Article 3 of the DMA, a gatekeeper is a platform that provides core services, has a significant impact on the internal market, and enjoys a stable and entrenched position as an intermediary between users and businesses. In practice, firms like Meta, Google or Apple meet these criteria due to their scale, integration, and ability to set the terms of access for others (European Commission, 2022; Danois, 2024).

Interoperability, as defined in Article 2(29), refers to the capacity of different systems to work together. The DMA requires, for example, that messaging services owned by gatekeepers become compatible with third-party platforms upon request (Article 7). This is intended to reduce switching costs and allow for more multi homing**,** enabling users and businesses to operate across several ecosystems (Frison Roche and Roda, 2022). Although technically complex, this obligation aims to break down barriers that prevent competition and to open closed networks to alternative providers.

On the fairness front, the DMA introduces obligations that rebalance power between dominant platforms and business users. Gatekeepers must share user interaction data with the businesses that generate it (Article 6(1)(i)), ensure non discriminatory access to advertising tools (Article 5(9)), and allow firms to communicate with their customers freely, even outside the platform (Article 5(4)). These rules target structural dependencies that limit firms' strategic autonomy and visibility (SopR2fep, 2022).

This framework reflects a logic of asymmetric regulation, applying strict obligations only to dominant actors, rather than uniformly across all platforms. As Roda (2022) explains, this approach is designed to preserve flexibility for smaller firms while reinforcing contestability at the heart of digital ecosystems. However, scholars such as Schweitzer et al. (2021) point out that effective enforcement is essential. Inconsistent regulatory efforts, such as those observed in Ireland, where several gatekeepers are headquartered, risk weakening the overall ambition of the regulation (Valletti and Zingales, 2021).

2.2.3. Assessing the Economic and Technological Impacts of the DMA: Insights from Early Studies

The adoption of the Digital Markets Act has triggered considerable academic and institutional analysis regarding its effects on the structure of digital markets and the broader technological landscape within the European Union. As the first comprehensive tool of ex ante regulation in this domain, the DMA stands apart from traditional competition law and invites early assessments of its expected outcomes, despite the absence of long-term empirical data.

Economically, the most frequently cited objective of the DMA is to enhance market contestability. By addressing practices that reinforce the dominance of a few platforms and by facilitating access to data and key platform functionalities, the regulation aims to create new opportunities for small and medium-sized firms. The Panel of Economic Experts (2021) suggests that lower switching costs, combined with increased transparency, could allow alternative providers to compete on more equal footing, particularly in sectors such as advertising, app distribution, or cloud infrastructure. In these contexts, access to a large user base and to aggregated data flows has historically created a strong structural advantage for gatekeepers (Larouche and de Streel, 2021).

From a technological standpoint, the DMA introduces significant requirements that may alter the internal architecture of platforms. Rules related to interoperability**,** data portability**,** and real-time auditability may compel gatekeepers to redesign elements of their systems. Ensuring compatibility between messaging services, while maintaining

encryption and performance standards, raises complex challenges in terms of security and scalability (Roda, 2022). The same applies to the obligation to separate data silos, which could undermine some of the technical synergies that large platforms have built over time.

Nevertheless, several studies point to possible short-term drawbacks. High compliance costs could lead to increased prices for downstream services or reduce investment in certain areas, particularly those dependent on economies of scope and data integration (Monti, 2021; Ibáñez Colomo, 2021). Moreover, rigid implementation of technical standards may limit the ability of platforms to iterate and innovate rapidly, especially in emerging fields such as artificial intelligence or personalised content.

The impact on innovation ecosystems remains debated. While some researchers argue that the DMA will revitalise competition and encourage more diverse forms of digital innovation (Akman, 2021), others suggest that the additional legal uncertainty may encourage conservative strategies, especially among large incumbents. The long-term effect for startups depends largely on the degree of regulatory consistency across Member States and the effectiveness of institutional enforcement mechanisms (Schwab, 2021). Beyond Europe, the DMA may have extraterritorial effects. Many scholars refer to the Brussels effect, whereby non-European firms choose to adopt EU standards globally to avoid the cost of segmentation. If this dynamic materialises, the DMA could indirectly shape platform governance far beyond European borders and influence global regulatory norms (Monti, 2021).

2.3. General Data Protection Regulation (GDPR)

2.3.1. Strengthening Personal Data Protection & User Rights and Business Obligations

The General Data Protection Regulation (GDPR), enforced since May 2018, redefined the legal framework for protecting personal data within the European Union. Its goal is twofold: it aims to safeguard fundamental rights, in particular those stated in Article 8 of the Charter of Fundamental Rights of the EU, and to ensure the free movement of data within the single market (Voigt & von dem Bussche, 2017).

To achieve this, the GDPR relies on core principles such as lawfulness, fairness**,** transparency**,** data minimization**,** and purpose limitation (European Union, 2016, Art. 5). A key innovation is the principle of proportionality, which requires that data processing be limited to what is strictly necessary for a clearly defined purpose (Bulgakova, 2023). This is especially important for sensitive data like health, religious beliefs or biometric identifiers, whose use is generally prohibited except under specific legal grounds outlined in Article 9(2). The regulation reinforces several user rights, including access to one's data (Art. 15), rectification (Art. 16), erasure (Art. 17), data portability (Art. 20), and objection (Art. 21). These rights increase individual control over digital identity and make it possible to contest certain forms of data use (Heimes, 2018).

On the organizational side, compliance is structured around key obligations. Article 25 requires privacy by design and by default, while Article 35 mandates Data Protection Impact Assessments (DPIAs) for high-risk processing. Article 37 requires companies in many sectors to appoint a Data Protection Officer (DPO). These mechanisms contribute to a broader shift toward accountability, where firms must be able to demonstrate their compliance efforts (Voigt & von dem Bussche, 2017, see Figure B.4.).

The GDPR also allows voluntary certification under Article 42. The scheme known as GDPR-CARPA enables organizations to certify their privacy practices through external audits. Although its uptake remains limited, it represents a tool to build legal credibility and user trust (Tikkinen-Piri et al., 2019).

2.3.2. Analysis of the identified impacts on data governance and innovation

Since its entry into force, the GDPR has significantly changed how organizations approach data governance and innovation. It requires firms to treat personal data as a strategic resource, with structured processes for collection, storage, use, and deletion. According to Hoofnagle, Van der Sloot, and Zuiderveen Borgesius (2019), this has led to the institutionalization of governance tools such as the appointment of a Data Protection Officer (DPO), the implementation of Data Protection Impact Assessments (DPIAs)**,** and reinforced internal compliance mechanisms.

Financial risk has also become a central factor. With fines of up to 4% of global turnover, many firms have adopted compliance-by-design models, incorporating privacy into their product development and operations. Ferrara, Faggiani, and De Gregorio (2017) point out that this often translates into deeper organizational learning and the integration of data protection into corporate social responsibility strategies. Still, the level of adaptation varies depending on the sector and size of the company. On the innovation side, the impact remains mixed. Several empirical studies, including those by Von Blumenthal et al. (2022) and Jia, Jin, and Wagman (2021), highlight how small and medium-sized enterprises (SMEs) often see the regulation as a constraint. Many reports having delayed digital projects, redirected budgets toward legal advice, or limited experimentation due to the complexity of compliance.

However, the GDPR has also stimulated new forms of compliance-driven innovation. Martin et al. (2019) distinguish between responses that either restrict or enable innovation. Some startups reduced their dependence on third-party data or personalization, while others created privacy-enhancing technologies such as differential privacy, local data processing, or anonymization tools. In sectors like finance and health technology, strong compliance is increasingly used as a signal of trust.

This aligns with the Porter Hypothesis, which suggests that well-designed regulation can drive firms to improve performance and develop solutions aligned with societal values (Arcuri, 2020). In particular, the telecommunications and ICT sectors have leveraged the GDPR to build secure systems, enhance consent management, and redesign interfaces with privacy by default principles (Cisco, 2019). The regulation also reshapes competitive dynamics. By enforcing data portability and restricting forced consent mechanisms, as outlined in Article 7(4), it challenges the dominance of large digital platforms and seeks to reduce lock-in effects (Grundmann & Hacker, 2020). Yet in practice, the adoption and enforcement of these mechanisms remain uneven across the EU.

2.3.3. Research on the concrete outcomes since its entry into force

Five years after its application, the GDPR has generated measurable but uneven outcomes within the European digital ecosystem. Among the most studied aspects is the implementation of Article 15, which grants individuals the right to access their personal data. In a comparative study of 21 websites from various industries, Pöhn, Mörsdorf, and Hommel (2023) observed that many companies still process access requests manually, often exceeding the one-month legal deadline. In several cases, the data was delivered in non-machine-readable formats, in contradiction with the data portability obligations defined in Article 20.

Rather than simple neglect, these shortcomings often reflect the operational difficulty of interpreting and applying complex legal standards. Pöhn et al. (2023) documented ten recurring dark patterns encountered by users, such as vague answers, unjustified refusals, or excessive identity verification. These findings illustrate the gap between the legal existence of user rights and their practical enforceability.

The effectiveness of regulatory enforcement has also been called into question. Buckley, Caulfield, and Becker (2024) conducted 70 interviews with industry experts and legal practitioners to assess the performance of DPAs. They found that while expectations are high regarding strategic enforcement and structural oversight, many national authorities lack resources and investigative capacity. In particular, the Irish Data Protection Commission (DPC), responsible for supervising firms like Meta and Google, has faced criticism for procedural delays and limited transparency in cross-border cases.

These findings suggest that the success of the GDPR depends not only on the legal text but on its institutional implementation. Structural disparities between Member States, especially in terms of funding and staff, lead to inconsistent interpretations and enforcement of the regulation across the EU (Buckley et al., 2024).

At the firm level, compliance strategies vary considerably. While many companies have formalized data governance through internal policies and legal departments, this does not always ensure consistent protection of data subjects. As Hoofnagle et al. (2019) highlight,

the existence of compliance structures does not necessarily translate into effective privacy practices. The internalization of GDPR principles depends heavily on the sector, the size of the company, and its business model.

2.4. Interaction Between the DMA and GDPR

2.4.1. Convergence points: Transparency and accountability of stakeholders

The Digital Markets Act and the General Data Protection Regulation are two essential instruments of the European Union's digital regulatory framework. The DMA focuses on promoting contestability and addressing imbalances caused by dominant gatekeepers, while the GDPR aims to protect fundamental rights by regulating how personal data is handled. Although they emerge from different legal traditions, these two texts converge on core principles such as transparency and accountability.

Transparency is a central requirement in both frameworks. Under the GDPR, organisations must clearly inform individuals about how their personal data is collected, used, and shared. The DMA reinforces this approach by obliging gatekeepers to communicate key information to their business users, such as advertising performance metrics or criteria used in ranking algorithms. This common effort helps reduce information asymmetry and enables more balanced relationships between platforms and those who depend on them (Geradin, Bania and Karanikioti, 2022).

The principle of accountability is also shared. The GDPR requires that data controllers implement internal measures to prove their compliance with data protection obligations. The DMA adopts a similar logic by demanding that gatekeepers establish internal procedures to monitor and report their own compliance. In both cases, the focus is not only on respecting the rules but also on demonstrating that those rules are actively upheld (Bieker, Podszun and Weigl, 2023).

Another area of alignment lies in the promotion of data portability. The GDPR grants individuals the right to transfer their data between services. The DMA reinforces this right by requiring gatekeepers to provide continuous and real-time access to relevant data in a

format compatible with the GDPR. This increases user empowerment and helps reduce the lock-in effects often seen in digital ecosystems (Weigl, Bieker and Podszun, 2023).

Finally, both texts impose restrictions on the cross-use of personal data. The GDPR limits such practices through rules on purpose limitation and explicit consent, while the DMA explicitly prohibits gatekeepers from combining personal data across services without valid user approval. These provisions aim to prevent the accumulation of large volumes of personal data that can be used to reinforce platform dominance (D'Amico, 2024). Together, the DMA and the GDPR reflect a consistent European regulatory vision. They are rooted in different domains but promote the same goals of transparency, fairness, and greater control for users and business actors operating within digital markets.

2.4.2. Points of tension: Interoperability versus data protection

Although the Digital Markets Act and the General Data Protection Regulation pursue complementary goals, their intersection reveals a number of tensions. The DMA promotes interoperability between platforms to enhance contestability, while the GDPR limits the circulation and processing of personal data to preserve user privacy. These objectives are not always easy to reconcile in practice. One of the clearest examples is the DMA's requirement for gatekeepers to make their services interoperable with third parties, especially in messaging. While this provision aims to reduce lock-in effects and foster competition, it often implies sharing personal data with external services whose data protection practices may differ. According to Martin-Lafay (2024), this creates risks in terms of lawful processing and user control.

Under the GDPR, personal data must be processed for specific purposes and only when a clear legal basis is established. However, interoperability may blur responsibilities between platforms, making it unclear who is the data controller and who is accountable for potential misuse (Weigl, Bieker and Podszun, 2023). This can weaken user rights such as access or erasure.

Another issue is the sensitivity of the data involved. Messaging content may include health or political information, which requires higher protection under Articles 9 and 32 GDPR. Yet, the DMA's requirements do not systematically distinguish between types of data (Reis, 2021).

Finally, enforcement fragmentation adds complexity. The DMA is handled by the European Commission, while the GDPR falls under national Data Protection Authorities. This dual oversight can lead to inconsistent interpretations and enforcement gaps (Geradin, Bania and Karanikioti, 2022). Some researchers have suggested that privacy-enhancing technologies such as federated learning, homomorphic encryption, or differential privacy could help reduce these tensions by enabling data sharing without revealing identifiable information (Podszun et al., 2021). Although promising, these tools remain difficult to apply at scale.

In short, while interoperability can enhance innovation and competition, it must not compromise the fundamental rights guaranteed by the GDPR. Achieving a functional balance requires clearer legal guidance and strong technical safeguards.

2.4.3. Research and gaps in the study of their interaction

Although the DMA and the GDPR are now central pillars of the European Union's digital policy, research on how these two instruments interact remains fragmented and underdeveloped. The complexity of their articulation, which touches on legal, technical, economic, and behavioural dimensions, makes it particularly difficult to build an integrated analytical framework.

One of the main research gaps concerns the absence of a coherent enforcement architecture. While several studies have identified tensions between interoperability and privacy (Bieker et al., 2023; Kara et al., 2023), there is still no concrete institutional model for resolving conflicts when obligations from both regulations overlap. In practice, there is no formal coordination between the European Commission, responsible for the DMA,

and national Data Protection Authorities, in charge of the GDPR, despite the growing number of cases that require joint interpretation (Kpeme and de Streel, 2024).

Another major limitation lies in the lack of empirical research. Most academic work to date has remained theoretical, with little attention to how gatekeepers actually implement obligations under Article 6 and 7 of the DMA while ensuring compliance with the GDPR. For instance, it remains unclear how platforms adapt internal governance structures to ensure that data sharing**,** user consent, and data minimisation coexist in complex operational settings such as messaging services or advertising ecosystems (Carabin, 2022).

There are also significant conceptual tensions. The DMA promotes data portability and system-wide interoperability to encourage market openness, whereas the GDPR aims to restrict data flows to protect user rights. This creates a normative tension that few legal scholars have addressed in detail. As noted by Weigl, Podszun and Bieker (2023), the principles of purpose limitation and data minimisation are difficult to reconcile with the systemic sharing and real-time access required by the DMA.

On the technical front, although many propose privacy-enhancing technologies as a bridge between the two texts, there is limited analysis of their concrete application. Solutions such as federated learning, homomorphic encryption, or pseudonymisation protocols are often cited, but rarely studied in the context of the regulatory obligations imposed by both the DMA and the GDPR (Martin-Lafay, 2024; EDPS, 2020). More work is needed to test their viability in real-world business contexts.

Lastly, the academic literature lacks a long-term theoretical framework to analyse how the interaction between these two regulations will evolve. The GDPR has already produced jurisprudence and regulatory practice since 2018, while the DMA is only beginning to be applied. Yet few longitudinal studies anticipate how these frameworks will converge or conflict in the future, especially in relation to emerging laws such as the Digital Services Act and IA Act(Nielson, 2024).

In light of these gaps, there is room to propose new models of integrated governance, for example through joint guidance from the European Commission and the European Data Protection Board. Similarly, future research could focus on identifying business sectors where the overlap is most operationally problematic, such as cloud services, digital advertising, or cross-platform communication tools. More importantly, interdisciplinary research that blends legal analysis, data engineering, behavioural economics, and platform strategy could help create a more holistic understanding of how to regulate powerful actors without weakening the rights of users. In short, addressing these gaps is not only an academic necessity, but a political one. Without a clearer understanding of how to align the DMA and GDPR in practice, there is a risk of fragmented enforcement, legal uncertainty for firms, and ultimately, diminished trust in the European digital regulatory framework.

3. Methodology Framework

3.1. Research design and data collection strategy

This research is based on a qualitative and exploratory approach. The aim is to examine how the interaction between the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA) influences business models and innovation strategies among firms operating in European digital markets. Rather than measuring regulatory effects through quantitative indicators, this study seeks to explore the way different actors perceive, interpret, and respond to these regulations. According to Denzin and Lincoln (2018), qualitative research is particularly suited for understanding the meanings individuals or groups assign to complex processes and environments, especially when dealing with evolving policy frameworks and organizational adaptation.

The study adopts a constructivist and interpretivist epistemological stance. It considers that knowledge of regulatory impact is shaped through experience, institutional discourse, and strategic decision-making. As Bryman (2016) points out, this approach aims to reconstruct how actors make sense of constraints and opportunities within a regulatory environment, particularly when legal texts generate tensions or require

strategic trade-offs. The thesis therefore focuses on collecting a diversity of informed perspectives across institutional, academic, and corporate domains.

The primary method used for data collection is semi-structured interviews. As suggested by Miles, Huberman, and Saldaña (2014), this method combines thematic consistency with flexibility, allowing interviewees to develop their arguments while enabling the researcher to follow up on relevant themes. This format is particularly relevant for capturing perceptions on topics that are still under development, such as the interpretation of the DMA in practice, or the institutional friction between privacy and interoperability provisions. Interviews were conducted individually, recorded with informed consent, and manually transcribed. Anonymity was granted where requested, and no personal data was retained.

Participants were selected using purposive sampling, based on their relevance to the research question and their professional or academic position within the regulatory, legal, or digital business ecosystem. The interview plan was built around the three analytical dimensions of the thesis: regulation, technology, and business strategy. Some profiles were contacted but could not participate due to scheduling constraints or lack of response. Nonetheless, four interviews were successfully conducted, providing complementary insights across the regulatory and business dimensions of the thesis. The table below summarizes the interview strategy and indicates the section of the thesis to which each respondent contributes (see Figure B.5.).

3.2. Interview design and analytical contribution

The interviews conducted for this thesis followed a semi-structured format, based on three thematic pillars: regulation, technology, and business strategy. An interview guide was developed to ensure consistency while allowing flexibility depending on the profile of the respondent (see Appendix C). Questions were grouped into three main areas. The first section explored the participant's understanding of the GDPR and the DMA and their respective rationales. The second focused on the practical implications of these regulations, with an emphasis on tensions or overlaps. The third addressed strategic or

organisational adaptation, particularly in relation to innovation and compliance. Each interview was tailored to the background and expertise of the participant, with some emphasis adjusted according to their role. This allowed the conversations to remain open-ended while ensuring that all core themes relevant to the research question were addressed. The use of semi-structured interviews was particularly appropriate given the relatively recent implementation of the DMA and the interpretative nature of GDPR enforcement, which require a contextual and experience-based exploration rather than a purely descriptive one.

Beyond the structural logic of the interviews, the choice of participants was guided by their potential to inform specific aspects of the research question. Each respondent provided a unique perspective that supported one or more sections of the thesis (see Appendix D). To better understand how the interaction between the GDPR and the DMA affects business models and innovation strategies in the European digital environment, a diverse set of interview profiles was selected. Each participant was chosen to contribute insight into a specific regulatory, strategic, or operational perspective. The selection aimed to capture the viewpoints of academic experts, institutional actors, business professionals, and, where possible, representatives of consumers and the media.

The professor of European law provided essential academic grounding on the legal architecture and interpretive tensions between the GDPR and the DMA. His expertise helped clarify enforcement gaps, overlaps between the two texts, and institutional coordination challenges. This was particularly valuable for understanding how legal uncertainty may affect compliance decisions.

The EU official contributed a regulatory perspective on the implementation of the GDPR and the interaction with other digital regulations. His insights helped explain how data protection rules are enforced in practice, how interoperability is interpreted by regulatory bodies, and how institutions attempt to balance innovation and privacy. This interview directly supported the regulatory analysis developed in the second chapter.

The journalist from Euractiv was selected for his expertise in covering European tech policy. The interview could not be realised, but the rationale for inclusion was to understand how these regulations are debated and communicated within the EU bubble. Such a media-based perspective would have contributed to evaluating how narratives influence the strategic framing of regulatory obligations by firms.

The professor in innovation strategy was interviewed to examine how firms adapt their business models under regulatory constraint. He provided analytical frameworks for understanding compliance-driven innovation, strategic positioning in regulated markets, and the role of legal uncertainty in shaping technological choices. His input was directly used to analyse how innovation is affected in chapter three.

The security manager at Elium, a mid-sized European technology company, offered a concrete view of how GDPR and DMA compliance is implemented operationally. His testimony illustrated how legal requirements are translated into product and process design, especially regarding data minimisation and platform interoperability. This practical perspective helped ground the more theoretical arguments in real-world organisational practices.

Additional profiles were selected to further enrich the diversity of views but could not be reached. A representative from Google was targeted to reflect the perspective of a gatekeeper subject to the DMA. A representative from Odoo was chosen to understand how small and medium-sized enterprises integrate regulation into their growth strategies. Mistral AI was selected to capture the experience of a European start-up operating in a high-regulation and high-innovation sector. Finally, BEUC and Test Achats were approached to represent consumer organisations, whose views would have helped assess whether these regulatory frameworks effectively protect user rights and improve the digital experience for citizens.

Each of these interviews, whether realised or not, was part of a deliberate methodological strategy designed to approach the research question from multiple, complementary angles. After transcription, all interview data were analysed through manual thematic

coding. Categories were created inductively based on emerging ideas and recurring patterns. These were then grouped into broader analytical dimensions, such as legal uncertainty, compliance adaptation, and innovation under constraint. In parallel, triangulation with academic literature and official reports helped validate interpretations and highlight points of convergence or divergence between different actors' perspectives. This integrated and comparative reading of the material ensures that the research findings reflect not only the individual narratives of each participant but also the broader strategic and regulatory tensions at the heart of Europe's digital transition. Every interview and transcription can be found in the appendix of this thesis.

4. Analysis of the results

4.1. Analysis of Technologies and Market Challenges

4.1.1. Technological Landscape

The current digital infrastructure in Europe is structured around a limited number of dominant global players. These include large technology companies such as Google, Amazon, Apple, Meta and Microsoft, which operate essential services such as search engines, operating systems, app stores, cloud platforms and communication tools. These services serve as critical intermediaries in the digital economy and increasingly influence how users access information, services and markets. The digital ecosystem is further shaped by emerging technologies such as artificial intelligence, biometric data processing, immersive platforms and decentralised architectures, all of which pose new challenges for regulation and compliance.

According to a senior official interviewed (anonymus) for this thesis, the GDPR was deliberately designed to be neutral with regard to technology. This means its provisions apply across all sectors and digital tools as long as personal data is processed. However, the official also acknowledged that some technologies have reached such a degree of complexity that they require dedicated regulatory responses. In particular, artificial intelligence systems are viewed as requiring additional rules that clarify how GDPR principles apply to machine learning, automation and opaque data processing models (Interview with EU official, 2025). The DMA addresses a different set of problems but

often targets the same technological environments. It focuses on firms that act as systemic intermediaries and concentrates on market power, interoperability restrictions and the misuse of data across services.

The DMA identifies core platform services such as operating systems, online marketplaces, advertising networks, browsers, virtual assistants and cloud services. These technologies are considered critical because they serve as gateways to the digital economy. The GDPR, in contrast, applies to all data processing operations and is particularly relevant for technologies that involve the collection, analysis and transfer of personal data. As the EU official explained, many of the requirements found in the DMA are explicitly aligned with GDPR principles. For example, Article 5 of the DMA restricts the combination of personal data between services without valid consent. This reflects the same logic as the GDPR's approach to data minimisation and purpose limitation.

Some of the most sensitive technological practices identified by both legal frameworks include algorithmic profiling, behavioural advertising and lack of interoperability. These practices are central to the functioning of many dominant digital services and are deeply embedded in their technical architecture and economic models.

Professor Alain Strowel, in an expert interview, expressed concern about the growing reliance on self-regulation by large platforms. He stated: *« If regulation is left solely to the platforms themselves, it will be difficult to adequately take into account the fundamental rights of users»* (Interview with Alain Strowel, 2025). This is especially relevant in the case of artificial intelligence, where the opacity of decision-making systems often conflicts with the GDPR's requirements for explainability and user control.

Behavioural advertising is another key issue, particularly because it forms the basis of the revenue models for most free services. It relies on extensive tracking of user behaviour across websites, devices and applications. As explained by the EU official, this practice often involves combining data from different services and building user profiles that are used for targeted advertising. Under the GDPR, such processing typically requires explicit consent. The DMA reinforces this requirement by introducing additional restrictions on

how data can be reused between services, particularly when it comes to core platform providers with gatekeeping power (Interview with EU official, 2025).

Interoperability is a more recent focus of regulatory attention. Under the DMA, designated gatekeepers are required to ensure that their services can interact with third-party applications or systems when requested by users. This includes obligations for messaging platforms, app stores and operating systems. While the aim is to increase competition and user choice, interoperability also creates potential risks for privacy and security. Professor Strowel warned that forcing interoperability without proper safeguards could undermine data protection. In particular, if user data must flow between different services, it becomes essential to ensure that all parties comply with GDPR standards and that no data is shared beyond what is necessary (Interview with Alain Strowel, 2025).

To summarise, Europe's digital infrastructure depends on a tightly integrated network of platforms, services and data-driven technologies. The GDPR and the DMA both attempt to structure this ecosystem in ways that promote fairness, transparency and respect for user rights. However, the interviews suggest that the alignment between legal frameworks and technological realities remains difficult to achieve. Regulators face the ongoing task of adapting their enforcement strategies to keep pace with innovation, while companies must increasingly design their services in ways that account for both market obligations and privacy compliance.

4.1.2. Scenarios Without Regulation

Before the adoption of the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA), dominant platforms operated in a context where regulatory intervention was limited, fragmented, or entirely absent. This regulatory vacuum, both in pre-GDPR Europe and in non-EU jurisdictions, enabled a set of structural behaviours that would later become central concerns for European legislators. Among these were the exploitation of personal data without user consent, the use of technical lock-ins to reinforce market dominance, and the amplification of disinformation and manipulative content through opaque algorithmic systems.

In terms of data protection, the absence of harmonised legal obligations allowed major platforms to process user data with little oversight. A well-known example is the 2016 change in WhatsApp's privacy policy, which allowed user data to be shared with Facebook for advertising purposes. This happened despite previous assurances that the services would remain independent. At the time, European regulators lacked the legal tools to enforce restrictions on such cross-service data integration. As explained by a senior EU official interviewed for this thesis, "*Before the GDPR, there were mainly recommendations or codes of conduct, but very few binding mechanisms. A real legal lever was missing to compel platforms to comply with certain principles."* (Interview with EU official, 2025). This lack of enforceability created a gap between user expectations and actual practices, particularly when it came to informed consent and purpose limitation. The situation was similar outside the EU, where platforms like TikTok were criticised for collecting biometric data, tracking underage users, and transferring personal data to servers located in third countries, often without user awareness or legal safeguards.

The lack of a competition framework specifically adapted to digital ecosystems also facilitated abusive practices. Gatekeepers were able to favour their own services, restrict interoperability, and leverage user data to reinforce their dominance across multiple markets. As the EU official noted, "*The ability to combine data across services provided a huge competitive advantage, whether for targeted advertising or algorithmic optimisation. Without the GDPR or the DMA, there was nothing to prevent it*" (Interview with EU official, 2025). Meta's ability to integrate user data across Facebook, Instagram and WhatsApp exemplifies how technical integration and regulatory opacity can entrench dominance. Similarly, Amazon's dual role as both marketplace operator and competitor enabled it to use data from third-party sellers to inform the design and promotion of its own products. These forms of self-preferencing were difficult to address under traditional antitrust law, especially in the absence of transparency and interoperability requirements.

Risks related to manipulation, surveillance and algorithmic opacity were also exacerbated by the lack of regulation. Platforms optimised for engagement and retention often amplified controversial or misleading content, especially in politically sensitive contexts. Without external auditing or transparency requirements, recommendation algorithms

became black boxes that shaped public discourse without accountability. Professor Alain Strowel highlighted the dangers of relying solely on voluntary commitments from platforms in this area: « *If regulation is left solely to the platforms themselves, it will still be difficult to adequately take into account the fundamental rights of users* » (Interview with Alain Strowel, 2025). This concern extends beyond data protection into broader issues of digital governance, including content moderation, algorithmic fairness, and the democratic integrity of online information systems.

These examples help explain why the European Union progressively moved towards a dual regulatory approach. The GDPR was designed to restore users' control over their personal data and to impose clear obligations on data controllers. The DMA, in contrast, was introduced to tackle structural market failures caused by gatekeepers who control access to digital infrastructure. As the EU official explained, « *The GDPR protects the fundamental rights of the user, while the DMA targets the structural behavior of platforms. These are two complementary approaches, but they must be successfully coordinated* » (Interview with EU official, 2025). A comparative overview of the main issues described in this section is presented in the table below (see figure B.6.). It summarises how different platforms illustrate the types of harms that emerged in the absence of regulation and highlights which frameworks were lacking at the time.

4.2. Impact of European Regulations on Businesses and markets

4.2.1 Competitiveness and attractiveness

The dual regulatory framework introduced by the GDPR and the DMA has deeply reshaped the European digital economy in profound ways. While its stated goals are to enhance user rights, preserve fair competition, and foster a trustworthy digital environment, its impact on competitiveness remains subject to debate. This section explores whether these regulations strengthen or weaken the position of European firms relative to global competitors, and how they influence the attractiveness of the EU market for start-ups and investors.

One of the most frequently cited tensions lies in the asymmetry of compliance costs and capacities between large foreign platforms and European digital firms. The GDPR applies extraterritorially, meaning that non-European firms must comply with its provisions when processing data from EU citizens. However, in practice, as noted by the EU official interviewed for this thesis, « *Some large platforms have the legal and technical means to delay or adapt their compliance. This is not the same reality for European SMEs* » (Interview with EU official, 2025). This contrasts sharply with the experience of smaller European firms, who often act as regulatory takers, forced to comply with stringent rules without influencing their formulation.

This distinction is especially relevant in the case of start-ups. As the security manager from Elium explained, the GDPR has become « *A useful lever to strengthen, structure, and highlight principles we were already applying* », but it also imposes a heavy operational burden, particularly in managing subcontractors, documenting compliance, and adjusting technical architectures to local hosting and sovereignty expectations (Interview with Elium, 2025). While these requirements contribute to building trust and transparency, they also slow down product development and introduce scalability constraints, especially in the context of multi-tenant SaaS platforms. In the short term, these obligations can reduce agility and limit the adoption of third-party services that are commonly used by more flexible competitors outside the EU.

The situation is further complicated by the increasing expectations of European clients, especially in sensitive sectors such as public administration, finance, or healthcare. According to the Elium interviewee, « *Our clients express a strong demand: that their data not be processed or hosted by non-European companies* ». This leads to stricter scrutiny of data hosting, subcontracting chains, and even the legal jurisdiction of vendors. In response, companies like Elium have adapted their architecture to rely exclusively on European infrastructure providers, sometimes at the cost of technical flexibility or access to advanced global services.

Nevertheless, the perception of the GDPR and DMA is not uniformly negative. Both interviewees acknowledged that these frameworks have also created a competitive

differentiation opportunity for companies that position themselves as privacy-first and compliance-oriented. The Elium case illustrates this well. Their efforts to implement privacy by design, transparency clauses, and advanced traceability features have helped them win clients in highly regulated environments. As noted by the innovation professor interviewed, « *In certain market segments, compliance becomes a competitiveness factor in its own right, especially when trust is a decisive selection criterion* » (Interview with innovation expert, 2025).

The Digital Markets Act, although primarily targeting large gatekeepers, also influences the market environment for smaller firms. While it does not impose direct obligations on start-ups like Elium, it indirectly affects them through the expectations of their clients and the broader shift in platform governance. For example, increased pressure on gatekeepers to offer interoperability, fair access and transparency may open new integration opportunities or reduce dependency risks for B2B solution providers. However, this depends on effective enforcement and cross-regulation coordination.

Taken together, the European regulatory context presents a dual reality. On the one hand, it imposes significant short-term compliance costs and limits operational flexibility, especially for smaller actors. On the other hand, it fosters a framework of trust and credibility that can strengthen the long-term positioning of European firms, particularly in markets where data protection and sovereignty matter. The ability to turn these constraints into strategic assets differentiates regulatory takers from potential shapers**.** While many SMEs currently fall into the taker category, those who anticipate regulatory trends and embed compliance into their product DNA may gain a first-mover advantage in an increasingly privacy-conscious digital economy. A comparative summary of these dynamics is presented in the table below, contrasting compliance strategies and perceived impacts across different types of actors (see Figure B.7.).

4.2.2 Innovation and economic Models

The enforcement of the GDPR and the DMA has deeply affected how European digital companies design, deploy, and monetise their services. While regulation is often

perceived as a constraint to innovation, several interviewees stressed that it can also act as a lever for transformation, especially when firms adopt a proactive rather than reactive stance. This section explores the limitations imposed by regulatory frameworks on traditional data-driven models, and the emerging opportunities tied to privacy-oriented design and open source ecosystems**.**

The GDPR introduced strict requirements on data collection, processing purposes, and user consent. These rules challenge the viability of many traditional business models based on large-scale behavioural tracking and personalised advertising. For start-ups and SaaS providers, the ability to collect and use data is now constrained not only by legal boundaries but also by user expectations and contractual transparency. As noted by the innovation professor interviewed, « *Business models based on the intensive exploitation of personal data are becoming increasingly difficult to justify, especially in an environment where trust is a key factor of differentiation* » (Interview with innovation expert, 2025). This shift pushes companies to rethink their value proposition, moving away from data extraction and toward user empowerment, transparency, and modularity.

For smaller actors, these constraints can be particularly demanding. As the Elium security manager explained, « *The GDPR requires extensive documentation and traceability, which is burdensome to manage in an agile environment* ». These demands force engineering teams to integrate compliance mechanisms early in the development lifecycle, often through dedicated privacy impact assessments, traceability matrices, and role-based access control systems. While this increases initial development costs, it also reduces risks of legal non-compliance and builds trust with privacy-conscious clients. In Elium's case, the implementation of privacy by design and privacy by default was not only a legal obligation but also a differentiator that helped them win contracts in regulated sectors.

The notion of *privacy by design*, first introduced in the GDPR as a legal principle, has become a driver of architectural innovation. Companies like Elium have implemented features such as granular permission systems, real-time audit logs, and data localisation options to comply with both regulatory and client requirements. As the innovation professor stated, « *Compliance can become a source of product innovation if it is anticipated*

and integrated from the design stage ». This is a clear illustration of the transition from a reactive *regulatory taker* posture to a more strategic *regulatory shaper* approach. Firms that internalise regulatory constraints and use them as design inputs are better positioned to align with market trends and regulatory expectations.

This dynamic is also visible in the growing appeal of open source models within Europe. Projects like Mistral or Odoo illustrate how companies can build scalable platforms while remaining compliant with European values such as transparency, data sovereignty, and interoperability. As noted in the interviews, open source frameworks facilitate independent audits, foster developer communities, and provide an alternative to opaque proprietary systems. For companies subject to strict compliance clauses, especially in public procurement or health-related fields, the use of auditable and privacy-respectful technologies becomes a competitive asset.

Regulatory frameworks may also encourage architectural simplification and long-term resilience. In the words of the Elium interviewee, « *Integrating compliance into the product from the outset allows us to limit legal risks and avoid costly redesigns later on* ». Rather than retrofitting compliance onto existing architectures, forward-looking companies embed it into their core logic. This transition reflects a broader cultural shift in European digital innovation: from scale-first, data-intensive strategies to modular, accountable and sovereignty-aware models. However, this transformation is not without friction. Access to external services, particularly AI tools and cloud components, is increasingly limited by legal constraints regarding data transfer, hosting, and subcontracting. Companies must often weigh the innovation potential of new technologies against their compliance risks. Furthermore, the fragmentation of national interpretations of the GDPR can introduce uncertainty, particularly for companies operating across multiple member states. As the innovation professor warned, « *The real challenge is not regulation itself, but its local interpretation, which can unpredictably hinder technological adoption* ».

In conclusion, while the GDPR and DMA impose constraints on conventional data-driven business models, they also open a path for innovation based on user trust, legal alignment, and architectural transparency. Firms that adopt *privacy by design* and engage with open

ecosystems position themselves not only as compliant but also as credible and resilient. This orientation is increasingly shaping the identity of competitive European tech players who wish to remain autonomous from dominant global platforms and align with the evolving expectations of regulators, investors, and end-users alike.

4.2.3. Case Studies

The European regulatory framework has prompted highly differentiated responses from firms depending on their size, origin, regulatory exposure and strategic priorities. This section presents six contrasting case studies to illustrate how both global and European actors have adapted, either proactively or reactively, to the GDPR, the DMA and related legal instruments. The cases span sectors from digital platforms and messaging services to open-source AI and enterprise software.

Google News – Copyright, Competition, and National Interpretation:

The case of Google News in France and Belgium illustrates how EU regulation interacts with national copyright laws and market dynamics. Following the adoption of the EU Copyright Directive in 2019, France was the first country to transpose the neighbouring rights provision for press publishers. Google initially refused to pay for news snippets and removed preview content from its French results. This triggered an investigation by the French competition authority, leading to a 500 million euro fine and a forced negotiation process. Ultimately, Google accepted to remunerate publishers through the "News Showcase" initiative, but only after significant legal pressure. In Belgium, negotiations were less conflictual but revealed the same imbalance in negotiation power. This case demonstrates the regulatory shaper posture of Google, which sought to influence the regulatory outcome while minimising concessions. It also reveals the role of national authorities in interpreting and enforcing EU directives, often leading to uneven outcomes across member states.

Meta / WhatsApp – Consent Design and the Limits of Default Settings:

Meta's integration of WhatsApp into its data ecosystem has long been criticised for bypassing meaningful user consent. In its privacy policy updates since 2016, Meta

introduced changes allowing cross-service data sharing, often using pre-ticked boxes or ambiguous language. This approach exemplifies a regulatory taker posture: the company adapts its practices only when compelled by regulators. Although both the GDPR and DMA require clear opt-in consent for such data processing, Meta has continued to frame its consent mechanisms in ways that raise questions about freedom of choice and user understanding. As highlighted by the innovation professor interviewed, « *Default settings remain a very powerful strategic lever. As long as they are legally tolerated, they will be used* » (Interview with innovation expert, 2025). This case reveals the gap between legal compliance and user-centric design, and the challenge of enforcing meaningful default privacy protections in practice.

Mistral – Open-Source AI as Strategic Compliance:

Mistral, a French AI company founded in 2023, has embraced open source as both a technical philosophy and a regulatory hedge. By publishing its large language models openly and avoiding black-box architectures, Mistral positions itself as aligned with European values of transparency, auditability and sovereignty. While it remains subject to the GDPR and the upcoming AI Act, its privacy-by-default approach and refusal to engage in mass data collection distinguish it from US-based closed models. This proactive adaptation reflects a regulatory shaper posture, as Mistral seeks to influence the terms of the AI policy debate by offering a compliance-aligned alternative. As noted in several public statements, its strategy relies on trust-building with institutional clients and governments who are wary of dependency on American hyperscalers.

Odoo – Embedded Compliance in a European SaaS Model

Odoo, a Belgian enterprise software provider, offers a strong example of how regulatory compliance can be embedded into product architecture. Operating under a Software-as-a-Service (SaaS) model hosted entirely within Europe, Odoo structures its platform to align with GDPR principles such as data minimisation, access control and localisation. Its modular system allows customers to manage permissions and configure hosting preferences according to their internal policies. While no direct interview with Odoo was conducted at the time of writing, public documentation and strategic choices suggest a proactive stance towards compliance integration. Rather than retrofitting data protection

features, the company anticipates regulatory expectations and integrates them into its core offering. This positions Odoo closer to a *regulatory shaper* posture, showing how European software providers can transform legal constraints into product strengths and competitive differentiation.

Helium – Regulatory Pressure and the Strain of Dual Compliance

Helium, a small Belgian tech company, illustrates the challenges faced by SMEs in dealing with both GDPR compliance and specific client-imposed legal clauses. As explained by its security manager, Helium must comply not only with general European rules but also with highly customised requirements from clients in sensitive sectors. These include strict subcontracting controls, data localisation and contractual guarantees beyond regulatory baselines. « *Our clients sometimes request clauses that are more restrictive than the GDPR itself, particularly regarding data localisation or subcontracting* » (Interview with Elium, 2025). This reactive adaptation places Helium in a regulatory taker posture, where the cost of legal conformity can slow down product evolution and market expansion. However, the firm also leverages its European identity and its compliance transparency as trust-building tools in highly scrutinised procurement processes.

OpenAI / Claude / Gemini – Extra-European AI Strategies and Market Access

The deployment of US-based generative AI models such as OpenAI's GPT, Anthropic's Claude or Google DeepMind's Gemini has faced increased scrutiny in Europe. Concerns include the use of web scraping for model training, the lack of explainability and unclear data governance. In 2024, OpenAI temporarily restricted GPT access in the EU due to regulatory uncertainties related to the GDPR and the upcoming AI Act. These companies exemplify a regulatory taker posture from outside the EU, forced to adapt to a complex compliance landscape without shaping it directly. Their response has included geoblocking, reliance on European partners and selective deployment strategies. This raises critical questions about Europe's technological sovereignty and its ability to attract or retain cutting-edge technologies under a stringent regulatory regime.

4.3. Advantages and disadvantages of a strict Regulatory Framework

4.3.1. Advantages

The implementation of the GDPR and the DMA has created several tangible benefits for both businesses and consumers across the European Union. While the regulatory burden is often discussed in terms of constraints, many interviewees emphasized the strategic, operational and reputational advantages that stem from adopting a compliance-first approach.

Enhancing consumer trust and transparency

One of the most frequently cited benefits of the GDPR is its role in reinforcing user trust in digital services. The regulation grants European citizens concrete rights over their personal data such as the right to access, correct, delete, and port data, and it forces companies to adopt clearer and more user-friendly consent mechanisms. As the EU official explained, « *One of the most tangible effects of the GDPR has been the imposition of transparency standards that did not previously exist. Even non-European companies have partially adopted them to avoid appearing opaque in Europe* » (Interview with EU official, 2025).

Creating a level playing field and reducing market asymmetries

The DMA, though primarily aimed at curbing the dominance of gatekeeper platforms, also contributes to user empowerment by fostering fairer competition. Measures such as unbundling, default app changes, and restrictions on data combination create space for emerging players to enter the market. According to the innovation expert, these obligations « *make market entry conditions slightly less unequal* » for European firms that do not have the same access to user data or platform control as the large global incumbents (Interview with innovation expert, 2025).

Enabling compliance-driven innovation and differentiation

For some European firms, particularly start-ups and SaaS providers, regulatory compliance has become a strategic asset. Nicolas Parvais, security manager at Elium, noted that « *Our strategic choice to prioritise third-party services located in Europe [...] has*

helped strengthen our credibility with clients who are sensitive to these issues » (Interview with Elium, 2025). The company uses its full alignment with GDPR obligations including modular data architecture, auditability, and localisation as a competitive advantage in regulated industries. He also observed that « *Features initially developed to meet legal obligations turned out to be strong differentiating elements* ».

Encouraging internal maturity and operational resilience

Compliance with GDPR requirements has also led firms to formalise and structure internal processes, which strengthens long-term technical and organisational resilience. Elium highlighted that the GDPR encouraged better documentation, stronger governance practices, and traceability tools. As Parvais explained, this « *Also requires adopting a more structured and sustainable approach, which can become an advantage in terms of trust* ».

Shaping global standards and building reputational capital

Beyond the EU, compliance with GDPR is increasingly viewed as a mark of quality and accountability. The innovation professor interviewed emphasised that many European firms use GDPR alignment as a form of reputational capital. In his words, « *Some companies choose to comply first with European standards before expanding internationally. It is an investment in reputation, credibility, and trust* » (Interview with innovation expert, 2025). This aligns with the broader narrative of the GDPR and the DMA serving as instruments of regulatory influence beyond Europe's borders.

4.3.2. Disadvantages

While the GDPR and the DMA provide clear benefits in terms of legal harmonisation and digital sovereignty, the interviews conducted in this research highlight a number of drawbacks that impact the agility, scalability and competitiveness of European digital firms, especially for small and medium-sized enterprises.

Heavy compliance burden and resource asymmetry

One of the most cited limitations is the disproportionate compliance cost for smaller actors. Nicolas Parvais, security manager at Elium, noted that the regulatory framework

« *Imposes a high level of requirements [...] in terms of documentation, traceability, processing limitations, and subcontractor management. These obligations can lead to additional costs, lengthen development cycles, and hinder short-term innovation* » (Interview with Elium, 2025). While large multinationals can absorb such costs through internal legal departments and scalable infrastructure, smaller firms must divert a significant share of their resources to compliance, which can reduce their capacity to innovate or expand internationally.

Slowdown in product development and reduced flexibility

The GDPR's requirements on data minimisation, consent, and third-party vetting can limit technological flexibility. Parvais indicated that certain features had to be abandoned or delayed because they relied on third-party services hosted outside Europe. He explained that « *Some features that we could have developed quickly had to be redirected toward more compliant alternatives, which were sometimes less mature or more costly* » (Interview with Elium, 2025). This affects not only the speed of product rollout, but also the perceived competitiveness of European solutions compared to global alternatives.

Regulatory fragmentation and enforcement uncertainty

Although the GDPR is an EU-wide regulation, its enforcement remains uneven across member states. The innovation expert interviewed pointed out that « *The same rule can be interpreted differently by national authorities, which complicates matters for companies operating at the European level* » (Interview with innovation expert, 2025). This situation generates legal uncertainty and can deter cross-border expansion, especially for start-ups that cannot afford high legal consultation costs. The EU official also acknowledged that « *there are still coordination challenges between national DPAs and European institutions, and it slows down both enforcement and trust* » (Interview with EU official, 2025).

Risk of innovation deterrence in high-potential sectors

The cumulative weight of GDPR, DMA, DSA and the upcoming AI Act is sometimes seen as overly restrictive in emerging sectors such as artificial intelligence. As the innovation expert explained, « *We are trying to regulate uses we do not yet fully understand. In this context, some innovations simply will not emerge in Europe* » (Interview with innovation

expert, 2025). Alain Strowel echoed this concern, noting that « *Care must be taken not to hinder certain innovations in the name of a poorly calibrated precautionary principle* » (Interview with Alain Strowel, 2025). This risk is particularly relevant for AI systems based on data-driven learning or algorithmic experimentation, which face both legal and ethical uncertainties under the current framework.

Structural disadvantage versus global competitors

From a strategic standpoint, both interviewees acknowledged that the current framework puts European firms in a position of regulatory takers, forced to operate under stricter norms than their foreign competitors. Parvais emphasized that « *Small businesses and startups [...] are subject to the same obligations, which creates significant budgetary constraints* » (Interview with Elium, 2025). The EU official also recognized that « *many non-European companies adjust the minimum necessary to keep access to the market, while EU companies must go all-in to remain credible locally* » (Interview with EU official, 2025). This creates a competitive asymmetry where regulation, instead of fostering innovation, becomes a hurdle to it.

These regulatory dynamics create multidirectional effects across stakeholder groups. The following figure summarises how the GDPR and the DMA affect consumers, SMEs, large platforms and regulators, highlighting both tensions and potential synergies (see Figure B.8.).

4.3.3. Global Perspectives

The regulatory path chosen by the European Union, through the GDPR and the DMA, stands out in the global digital landscape. Unlike other major powers such as the United States or China, the EU has deliberately adopted a rights-based model, focused on individual freedoms, transparency, and accountability. This approach has not only shaped the internal digital market but has also positioned the EU as a normative force beyond its borders.

According to the EU official interviewed, the GDPR has given rise to a “soft power” dynamic. He explained that « *The GDPR imposes a model that, beyond Europe, is being reused on other continents. There is a kind of soft power spreading [...] companies based in Europe also ensure compliance with regulations inspired by the GDPR* » (Interview with EU official, 2025). This reflects what is commonly referred to as the Brussels Effect, through which European regulation influences global practices, especially among companies seeking access to the EU market.

In contrast, the United States follows a much more fragmented and market-led approach. There is no single federal law comparable to the GDPR, and regulatory responsibility is often left to the states or sector-specific agencies. This legal looseness encourages rapid experimentation, particularly in emerging fields like artificial intelligence. As the innovation expert put it, «*There is greater tolerance for experimentation in the United States. In Europe, we tend to think first before acting* » (Interview with innovation expert, 2025). That cultural difference may partly explain why the US remains home to many of the world’s largest and most agile tech firms, even if at the cost of weaker safeguards for users.

China, on the other hand, represents a third model centralised, state-driven, and strategically aligned with national objectives. It combines massive investment in emerging technologies with strong control over data flows and online content. While this model raises serious concerns about freedom and surveillance, it is also remarkably efficient in fostering large-scale digital innovation. The innovation expert observed that « *China is a good example. It is the opposite of liberalism, and yet it still innovates very effectively* » (Interview with innovation expert, 2025).

From the perspective of European firms, these differences create a complex environment to navigate. Compliance with EU standards is not always compatible with the requirements or practices of other jurisdictions. As the professor in innovation pointed out, the multiplicity of levels in Europe itself can be an obstacle: « *In Europe, I’m dealing with 27 countries, and then there are the regions, etc. [...] In the United States or China, I only*

have one interlocutor » (Interview with innovation expert, 2025). That structural fragmentation can act both as a protective buffer and as a brake on agility.

Despite this, the EU model remains a reference. Some firms see compliance with European rules as a badge of credibility. Others experience it as a constraint that limits their global reach. The innovation expert captured this duality well when he said, « *Europe's reputation as a leader in ethical regulation can become a strategic advantage [...] but it depends on the perspective* » (Interview with innovation expert, 2025). Whether the EU's influence will lead to greater convergence of digital norms or to deeper geopolitical fragmentation remains uncertain. What is clear is that Europe has chosen a deliberate path, one that prioritises rights, responsibility, and long-term trust over short-term disruption.

5. Conclusion

5.1. Summary of Findings

This thesis aimed to explore the extent to which the interaction between the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA) influences the business models and innovation strategies of European digital firms. Based on a qualitative approach combining academic literature, regulatory documents and expert interviews, the research sheds light on how these two frameworks shape the European digital ecosystem. The GDPR and the DMA were designed with different core objectives. The GDPR focuses on protecting individual rights related to personal data, while the DMA aims to restore market fairness and contestability in digital markets. Despite their different scopes, the research has shown that these two frameworks converge on several key dimensions, particularly concerning how data is collected, processed and monetised.

Findings demonstrate that compliance with both regulations creates a new strategic environment for companies. Some firms, especially large international platforms, respond with minimal legal adjustments to maintain market access. In contrast, many European SMEs and SaaS providers integrate compliance into their product architecture and corporate positioning. This divergence illustrates the distinction between regulatory

takers and shapers. At the same time, the GDPR has contributed to establishing the European Union as a global reference in digital governance. However, the ambition of these frameworks also creates friction, particularly in terms of operational complexity, legal uncertainty and regulatory fragmentation.

From my own perspective as a researcher, I consider the implementation of the GDPR and DMA to be not only necessary, but also beneficial for the future of European digital innovation. These frameworks offer a valuable opportunity for European companies, and especially start-ups, to distinguish themselves through transparency, user protection and responsible data governance. I see them as strategic tools that protect consumers while encouraging fairer competition. Far from being a hindrance, this regulatory environment can become a real competitive advantage for actors who align early and deliberately with these standards.

5.2. Recommendations

Several improvements can be proposed to enhance the implementation and impact of the GDPR and DMA. First, stronger coordination is needed between competition and data protection regulators, especially regarding practices such as self-preferencing, data sharing and interoperability. Second, small and medium-sized companies would benefit from simplified guidance, clearer documentation templates and tailored support to reduce the burden of compliance. Third, efforts should be made to harmonise regulatory interpretation across Member States to avoid fragmentation and legal uncertainty. Finally, the European Union should continue to invest in digital infrastructure and open-source innovation that align with the values embedded in its regulatory framework.

5.3. Limits of Paper

This research has several limitations that should be acknowledged. First, the number of interviews was limited, and some key actors declined to participate. Notably, no representatives from consumer organisations such as BEUC or Test-Achats responded, which left the consumer perspective underexplored. This is a significant gap, given that the ultimate purpose of both the GDPR and the DMA is to protect and empower users.

Second, despite outreach efforts, some firms such as Odoo, Google and Mistral did not take part in the empirical phase. Third, the recent nature of both regulations limits the availability of long-term impact data, and much of the enforcement activity and jurisprudence is still emerging. These factors restrict the scope of generalisation and make the conclusions of this study preliminary.

5.4. Future perspectives

This thesis offers a foundation for future academic exploration of the European digital regulatory model. A first avenue would be to incorporate the voice of consumers through interviews, surveys or collaborations with civil society organisations. A second direction would be to deepen the analysis by including perspectives from regulators and policymakers, especially those involved in cross-border enforcement or legal harmonisation. Third, future research could extend the regulatory scope by examining how the GDPR and DMA interact with other instruments such as the Digital Services Act and the Artificial Intelligence Act. Together, these frameworks will define the next phase of digital regulation in Europe and create new tensions and synergies. Finally, interdisciplinary approaches combining legal, technical and strategic perspectives could provide more actionable guidance for companies seeking to innovate responsibly in the European digital market.

References

- Akman, P. (2021). *Regulating competition in digital platform markets: A critical assessment of the framework and approach of the EU Digital Markets Act*. *European Law Review*, 46(5), 604–623.
- Autorité de la concurrence. (2021, July 13). *Droits voisins : sanction de 500 millions d'euros à Google*. Retrieved July 2025, from https://www.autoritedelaconcurrence.fr/
- Bieker, F., Podszun, R., & Weigl, A. (2023). *The DMA and the GDPR: Making sense of data accumulation, cross-use and data sharing provisions*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4460594
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
- Buckley, J., Caulfield, B., & Becker, S. (2024). *GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? Journal of Cybersecurity*, 10(1), tyad017. https://doi.org/10.1093/cybsec/tyad017
- Bulgakova, D. (2023). *The processing of personal data in accordance with the principle of proportionality under EU General Data Protection Regulation*. *Philosophy, Economics and Law Review*, 3(1), 266–284.
- Carabin, B. (2022). *The DMA's consent moment and its relationship with the GDPR*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4172582
- Commission européenne. (2022). *Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (Digital Markets Act)*. *Journal officiel de l'Union européenne*, L 265/1. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R1925
- Crémer, J., de Montjoye, Y.-A., & Schweitzer, H. (2020). *The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What is Fair*. European Commission. https://ec.europa.eu/info/publications
- DMA: Règlement. (2022). *Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 sur les marchés contestables et équitables dans le secteur numérique (Digital Markets Act)*. *Journal officiel de l'Union européenne*, L 265, 1–66.
- Danois, C. (2024). *Le Digital Market Act : Les mesures clés*. LEGITECH. https://www.legitech.lu
- Denzin, N. K., & Lincoln, Y. S. (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications.

- D'Amico, A. (2024). *Fragmenting consumer law through data protection and digital market regulations: The DMA, the DSA, the GDPR, and EU consumer law*. *European Law Journal*. Retrieved from https://onlinelibrary.wiley.com
- EDPS. (2020). *Response of the EDPS to the European Commission's consultation on the Digital Services Act package*. European Data Protection Supervisor. Retrieved from https://edps.europa.eu
- Elium. (2025). *Interview with the security manager of Elium conducted by Quentin Roland on 14 June 2025* [Unpublished interview transcript].
- Euractiv. (2024, June 3). *OpenAI temporarily blocks ChatGPT in EU over regulatory uncertainty*. Retrieved July 2025, from https://www.euractiv.com
- European Commission. (2022). *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925
- European Data Protection Board. (2023). *Binding decision 1/2023 on Meta IE*. Retrieved July 2025, from https://edpb.europa.eu
- Evangelista, R., Guerrieri, P., & Meliciani, V. (2014). *The economic impact of digital technologies in Europe*. *Economics of Innovation and New Technology*, 23(8), 802–824. https://doi.org/10.1080/10438599.2014.918438
- Evans, D. S. (2018). *Governing big tech: The law and economics of digital platforms*. Harvard Business Review Press.
- Evans, D. S., & Schmalensee, R. (2017). *Matchmakers: The new economics of multisided platforms*. Harvard Business Review Press.
- Evens, T. (2018). *Media economics and transformation in a digital Europe*. In L. d'Haenens, H. Sousa, & J. Trappel (Eds.), *Comparative Media Policy, Regulation and Governance in Europe: Unpacking the Policy Cycle* (pp. 41–54). Intellect.
- Ferrara, C., Faggiani, M., & De Gregorio, G. (2017). *Compliance e accountability nel nuovo Regolamento europeo sulla protezione dei dati personali*. *Law and Economics Yearly Review*, 6(2), 301–324.
- Frison-Roche, M.-A., & Roda, J. (2022). *L'interopérabilité comme outil de la régulation asymétrique des marchés numériques*. *Revue Lamy Droit de l'Immatériel*.
- Frison-Roche, M.-A., & Roda, J.-C. (2022). *Droit de la concurrence*. Dalloz.
- Geradin, D., Bania, K., & Karanikioti, T. (2022). *Mediating the tension between data sharing and privacy: The case of DMA and GDPR*. TILEC Discussion Paper.

- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). *Seeking qualitative rigor in inductive research: Notes on the Gioia methodology*. *Organizational Research Methods*, 16(1), 15–31. https://doi.org/10.1177/1094428112452151
- Grundmann, S., & Hacker, P. (2017). *Digital technology as a challenge to European contract law: From the existing to the future architecture*. *European Review of Contract Law*, 13(3), 255–293. https://doi.org/10.1515/ercl-2017-0012
- Grundmann, S., & Hacker, P. (2020). *Digital technology as a challenge to European contract law*. In *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 385–402). Cambridge University Press. https://doi.org/10.1017/9781108674385.025
- Heimes, R. (2018). *European Union General Data Protection Regulation (EU GDPR): What you need to know*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/en/knowledge/publications/51bb6f9b/european-union-general-data-protection-regulation
- Hoofnagle, C. J., Van der Sloot, B., & Zuiderveen Borgesius, F. (2019). *The European Union General Data Protection Regulation: What it is and what it means*. *Information & Communications Technology Law*, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501
- Ibáñez Colomo, P. (2021). *The Draft Digital Markets Act: A legal and institutional analysis*. *Journal of European Competition Law & Practice*, 12(7), 561–578. https://doi.org/10.1093/jeclap/lpab059
- Innovation Expert. (2025). *Interview with a professor in innovation conducted by Quentin Roland on 10 June 2025* [Unpublished interview transcript].
- Interview with EU official. (2025). *Semi-structured interview conducted by Quentin Roland on 12 June 2025* [Unpublished interview transcript].
- Iosifidis, P. (2002). *Digital convergence: Challenges for European regulation*. *Javnost - The Public*, 9(3), 27–47. https://doi.org/10.1080/13183222.2002.11008805
- Jia, J., Jin, G. Z., & Wagman, L. (2021). *The short-run effects of the General Data Protection Regulation on technology venture investment*. *Marketing Science*, 40(5), 671–691. https://doi.org/10.1287/mksc.2021.1294
- Kara, S., de Streel, A., & Kpeme, B. (2023). *Privacy considerations under EU competition law: The balance achieved in Article 5(2) of the Digital Markets Act and the effects of the Facebook decision*. Retrieved from https://papers.ssrn.com

- Klein, M. (2022). *Le Digital Markets Act (DMA) : Une nouvelle et importante étape dans la régulation européenne des acteurs du numérique*. *Institut Montaigne*. https://www.institutmontaigne.org
- Kpeme, B., & de Streel, A. (2024). *Institutional tensions between the European Commission and DPAs in the enforcement of digital regulation*. Centre on Regulation in Europe (CERRE).
- Larouche, P., & de Streel, A. (2021). *The European Digital Markets Act: A revolution grounded on traditions*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805280
- Lemoine, B. (2023). *Rapports de forces entre GAFAM et Union Européenne : Analyse de l'impact du Digital Markets Act sur la régularisation des plateformes digitales*. *Revue Concurrence & Régulation*, 2(11), 87–104.
- Martin-Lafay, M. (2024). *Étude sur l'interopérabilité impérative entre les plateformes de réseaux sociaux dans l'Union européenne*. Retrieved from https://ssrn.com
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.
- Mistral. (2024, October 9). *Announcing Mistral 7B*. Retrieved July 2025, from https://mistral.ai/news/announcing-mistral-7b/
- Monti, G. (2021). *The Digital Markets Act – Institutional design and suggestions for improvement*. *TILEC Discussion Paper No. 2021-006*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3788570
- Nielson, J. (2024). *Towards an integrated digital regulatory framework in the EU: Anticipating overlaps between the DMA, GDPR and DSA*. *Digital Policy Studies Review*.
- Nielson, N. (2024). *Vers un renouvellement de l'abus de position dominante face au défi de l'économie numérique ? Regards croisés entre droit antitrust américain et droit européen et interne de la concurrence* [Thèse de doctorat, Université Côte d'Azur]. HAL. https://theses.hal.science/tel-04931127
- OECD. (2019). *An introduction to online platforms and their role in the digital transformation*. OECD Publishing. https://doi.org/10.1787/53e5f593-en
- Odoo. (n.d.). *Odoo and the GDPR*. Retrieved July 2025, from https://www.odoo.com/page/gdpr
- Odoo. (n.d.). *Privacy Policy*. Retrieved July 2025, from https://www.odoo.com/privacy
- Panel of Economic Experts. (2021). *The EU Digital Markets Act: A report from a panel of economic experts*. European Commission. Retrieved from

https://op.europa.eu/en/publication-detail/-/publication/8ecbb40b-70ec-11ec-9136-01aa75ed71a1/language-en

- Petit, N. (2021). *The Draft Digital Markets Act: A Legal and Institutional Analysis*. *Journal of European Competition Law & Practice*, 12(6), 415–428. https://doi.org/10.1093/jeclap/lpab020
- Podszun, R., Bieker, F., & Weigl, A. (2021). *Régulations et protection de la vie privée: Une recherche hybride pour mieux appréhender les impacts sur le comportement des usagers du numérique*. *Zeitschrift für Datenschutz*.
- Pöhn, T., Mörsdorf, D., & Hommel, W. (2023). *Needle in the haystack: Analyzing the right of access according to GDPR Article 15 five years after the implementation*. *arXiv*. https://arxiv.org/abs/2308.15166
- Roda, J. (2022). *Éthique du numérique et marché : réflexions autour du Digital Markets Act*. *Revue Lamy Droit des Affaires*.
- Roda, J.-C. (2022). *L'interopérabilité comme outil de la régulation asymétrique des marchés numériques*. *Concurrences*, 1, 92–101.
- Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). SAGE Publications.
- Schwab, A. (2021). *Report on the proposal for a regulation on contestable and fair markets in the digital sector (Digital Markets Act)*. *European Parliament, Committee on the Internal Market and Consumer Protection (IMCO)*. Retrieved from https://www.europarl.europa.eu/doceo/document/A-9-2021-0332_EN.html
- Schweitzer, H., Haucap, J., Inderst, R., & Welker, R. (2021). *The EU Digital Markets Act: A Report from a Panel of Economic Experts*. Centre on Regulation in Europe (CERRE). https://cerre.eu/publications/the-eu-digital-markets-act-report-from-a-panel-of-economic-experts/
- SopR2fep. (2022). *Rapports de forces entre GAFAM et Union Européenne : Analyse de l'impact du Digital Markets Act sur la régulation des plateformes digitales*. *Revue du Droit Numérique*, 2(1), 34–52.
- Strowel, A. (2025). *Semi-structured interview conducted by Quentin Roland on 4 June 2025* [Unpublished interview transcript].
- The Art to Make Gatekeeper Positions Contestable. (2021). *An analysis of fairness and regulatory tools in the DMA*. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3846857

- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2019). *GDPR-CARPA: A look at the GDPR's first certification mechanism*. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 306–313). IEEE. https://doi.org/10.1109/EuroSPW.2019.00043
- Tóth, M., Dobrai, K., & Szabó, Z. R. (2022). *How data protection regulation affects startup innovation: Evidence from European startups*. *Journal of Innovation Management*, 10(3), 19–39.
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7
- Von Blumenthal, F., Blind, K., Gauch, S., & Hünermund, P. (2022). *The impact of the EU General Data Protection Regulation on innovation in firms*. *Research Policy*, 51(9), 104598. https://doi.org/10.1016/j.respol.2022.104598
- Wang, C., Zhang, N., & Wang, C. (2021). *Managing privacy in the digital economy*. *Fundamental Research*, 1(6), 543–551. https://doi.org/10.1016/j.fmre.2021.08.009
- Weigl, A., Bieker, F., & Podszun, R. (2023). *The interplay between the Digital Markets Act and the General Data Protection Regulation*. Retrieved from https://papers.ssrn.com
- Zandt, F. (2021, October 29). *Big Tech keeps getting bigger*. *Statista*. https://www.statista.com/chart/21584/gafam-revenue-growth/
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Appendix:

Appendix A: Glossary

Regulatory shaper

An actor that actively influences the design, interpretation, or implementation of regulation. These firms typically have the resources, scale, and institutional access to engage in lobbying, consultations, or technical standard-setting. In the context of the GDPR and DMA, regulatory shapers often include large digital platforms that help define compliance norms and influence enforcement practices across the digital ecosystem.

Regulatory taker

An actor that passively adapts to external regulation without participating in its development. This is often the case for smaller European firms, such as SMEs and startups, which must comply with frameworks designed by more dominant players. Regulatory takers have limited capacity to shape the rules but face the same legal and operational obligations under instruments like the GDPR and DMA.

Data sharing

The practice of making personal or non personal data accessible to third parties, including other firms, public bodies, or users, under specific legal, technical, and organizational conditions. In the context of the GDPR and DMA, data sharing must balance innovation and competition with privacy protection, often requiring mechanisms such as consent, pseudonymisation, or purpose limitation.

Interoperability

The capacity of different digital services, platforms, or systems to exchange data and function together without friction. Under the DMA, interoperability obligations aim to reduce lock in effects by enabling users and competing services to connect seamlessly with gatekeepers' ecosystems, such as messaging apps or operating systems.

Algorithmic transparency

The principle that automated decision making systems, such as recommendation engines or ranking algorithms, should be understandable, auditable, and accountable. This is increasingly demanded in both GDPR (in relation to profiling and automated processing) and DMA (regarding self preferencing or ranking criteria), as a way to enhance fairness, contestability, and trust in digital markets.

Technological platforms

Firms that provide a digital infrastructure enabling interactions between different user groups (e.g., buyers and sellers, app developers and users). They typically offer core functionalities like data processing, hosting, or application services and serve as a foundation for other digital activities to be built on.

Digital economy

An economy that is based on digital computing technologies, particularly the internet. It includes all economic activities that use digitized information and knowledge as key production factors.

GAFAM

An acronym for Google, Apple, Facebook (now Meta), Amazon, and Microsoft. Five of the most dominant U.S.-based technology companies with global reach. These firms are often discussed collectively due to their size, market power, and influence over key digital infrastructures.

Ecommerce

A system of buying and selling goods and services through digital platforms, especially over the internet. It includes both business-to-consumer (B2C) and business-to-business (B2B) transactions.

Operating systems

Software that manages computer hardware and software resources and provides common services for application programs. In mobile ecosystems, dominant operating systems include iOS (Apple) and Android (Google).

Social media

Digital platforms that enable users to create, share, or interact with content and to connect with other users. Examples include Facebook, Instagram, and TikTok. These platforms often monetize user data through targeted advertising.

API (Application Programming Interface)

A set of rules and protocols that allow different software applications to communicate and interact with each other. In digital ecosystems, APIs enable third-party developers to access certain functionalities or data from dominant platforms (e.g., payment systems, login services, geolocation). Restricting access to APIs can hinder innovation and reinforce gatekeeper control by limiting interoperability and excluding rivals.

Cloud computing

A model for delivering computing services (like servers, storage, databases, networking, software, and AI) over the internet on a pay-as-you-go basis. It allows firms to access scalable IT resources without owning infrastructure.

Multi sided market dynamics

An economic structure where a platform creates value by facilitating interactions between two or more interdependent groups (e.g., users and advertisers). Success on one side of the market often attracts more users on the other, generating network effects.

Network effects

A phenomenon where the value of a product or service increases as more people use it. In digital markets, strong network effects create significant barriers to entry for competitors.

Vertical integration

A business strategy where a company controls multiple stages of the supply chain or value chain. In the case of tech platforms, this may include owning the infrastructure (cloud), interface (OS), and content or services provided to end users.

Duopoly

A market structure dominated by two firms. In the context of mobile operating systems in Europe, Apple (iOS) and Google (Android) form a de facto duopoly by jointly controlling nearly the entire market.

Gatekeepers

Digital platforms that hold a structural position between businesses and end users, enabling them to control access to essential digital services. According to the DMA, gatekeepers have a durable position of power and set the rules of interaction within their ecosystems.

Digital Markets Act (DMA)

A European regulation adopted in 2022 that targets large online platforms designated as gatekeepers. It imposes obligations and prohibitions to ensure fair competition and prevent abusive practices before they occur (*ex ante* regulation).

Antitrust

A branch of competition law aimed at preventing anti-competitive behavior, such as market dominance abuse, collusion, or unlawful mergers. In the EU, it is enforced by the European Commission to maintain open and fair digital markets.

Economies of scale

Cost advantages that firms obtain as their production scale increases. In digital markets, platforms experience significant economies of scale by spreading fixed technology costs over a growing user base.

Data network effects

A type of network effect where increased usage of a platform leads to the collection of more user data, which in turn improves services (e.g., recommendations, personalization), making the platform even more attractive.

Algorithms

Sets of rules or instructions designed to solve problems or automate decision-making. In digital platforms, algorithms are used to rank search results, personalize content, or predict user behavior based on collected data.

Artificial intelligence (AI)

A field of computer science focused on creating systems capable of performing tasks that typically require human intelligence, such as learning, problem-solving, or pattern recognition. AI is widely used in digital platforms for personalization, automation, and predictive analytics.

Cloud providers

Companies that offer cloud computing services, including storage, processing power, and networking, via the internet. Major providers like AWS, Google Cloud, and Microsoft Azure host the infrastructure required for scalable digital services and AI training.

Technological sovereignty

The capacity of a nation or region to maintain control over its own technological infrastructure, data flows, and innovation pathways, without excessive reliance on foreign platforms or service providers.

Platform envelopment

A strategic practice where a dominant digital platform expands into adjacent or related markets to capture more user data, increase user dependency, and reduce multi-homing. This often blurs market boundaries and complicates regulatory intervention.

Open source

A type of software that is developed collaboratively and made freely available with its source code, allowing users to modify, distribute, or build upon it. Open source alternatives are often promoted for their transparency and independence from dominant platforms.

Targeted marketing

A marketing strategy that uses detailed user data to deliver customized advertising messages to specific audiences, increasing relevance and potential effectiveness.

Dynamic pricing

A pricing strategy in which the price of a product or service is adjusted in real time based on factors such as demand, competition, user behavior, or time of day.

Semi-structured interviews

A qualitative research method in which the interviewer follows a predefined guide of open-ended questions, while allowing flexibility to explore emerging themes and adapt the discussion based on the interviewee's expertise and responses. This approach balances consistency across interviews with the richness of spontaneous insights, making it particularly useful when studying complex or evolving phenomena, such as regulatory impacts on business models.

Lock-in effects

Situations in which users become dependent on a platform or service, making it costly or difficult to switch to alternatives due to data loss, network effects, or compatibility issues.

Qwant

A French-based search engine launched in 2013 that emphasizes user privacy by not tracking or profiling its users. It offers an alternative to dominant search platforms like Google by complying with European data protection standards and promoting ethical data use.

Nextcloud

A German cloud storage and collaboration platform that allows individuals and organizations to host their own private cloud services. Nextcloud positions itself as a secure, GDPR-compliant alternative to U.S.-based cloud providers, offering full control over data sovereignty.

Brave

A privacy-focused web browser that blocks ads and trackers by default. Brave also introduces an opt-in ad model that rewards users with cryptocurrency for viewing ads, aiming to offer a user-centric and transparent browsing experience.

Modular business models

Business structures that are composed of interchangeable and loosely connected components. They allow firms to remain strategically flexible by combining external platform benefits (such as reach) with internal control over core operations or services.

Opaque algorithms

Algorithms whose decision-making processes are not visible or understandable to users, regulators, or even developers in some cases. Their opacity raises concerns about accountability, fairness, and potential bias in digital services.

Ex ante rules

Regulatory measures that are applied proactively, before any harm or abuse occurs. In the context of the DMA, ex ante rules aim to prevent unfair behavior by gatekeepers rather than penalizing it afterward.

User choice

The ability of consumers to freely select between different digital services or providers. Preserving user choice is a central objective of competition and data protection policies in the EU.

Digital sovereignty

The capacity of a state or region to assert control over its digital infrastructure, data flows, and technological development, often in opposition to foreign dependencies on dominant non-EU tech firms.

Personal data

Any information relating to an identified or identifiable natural person, including names, emails, IP addresses, or browsing behavior. It is a foundational element in the functioning of the digital economy.

Privacy

The right of individuals to control the access, use, and sharing of their personal data. In the digital context, privacy is often challenged by extensive data collection and behavioral profiling.

Data protection

A legal and technical framework designed to ensure that personal data is processed securely, lawfully, and transparently. In the EU, it is primarily governed by the GDPR.

Power asymmetries

Situations where one party (often a digital platform) has significantly more information, control, or influence than another (typically users or small firms), leading to imbalances in market or data relationships.

Hyper personalized services

Digital services that are finely tuned to individual users based on real-time behavioral and contextual data, such as location, preferences, or past actions.

Predictive analytics

The use of statistical and machine learning techniques to forecast future behavior based on historical data. Commonly used in advertising, recommendation systems, and customer segmentation.

Targeted advertising

A marketing strategy that delivers advertisements tailored to specific users or user segments based on their interests, demographics, or online behavior.

Algorithmic decision-making

The use of automated systems or algorithms to make decisions that affect individuals or business processes, such as showing content, granting credit, or selecting job candidates.

Big data analytics

Techniques used to analyze extremely large datasets to uncover patterns, correlations, and trends that are valuable for business intelligence or decision-making.

Programmatic advertising

An automated method of buying and selling digital advertising space in real time, based on user data and bidding algorithms. It allows advertisers to target users with highly specific criteria.

Tracking technologies

Tools embedded in websites, apps, or emails to collect data on user behavior, such as cookies, web beacons, or device fingerprinting. Often used for analytics, personalization, or advertising purposes.

Informed consent

A principle in data protection whereby individuals must be fully aware of what data is being collected, how it will be used, and by whom, before agreeing to share it. It must be freely given, specific, informed, and unambiguous, according to the GDPR.

Data-driven business models

Business strategies that rely heavily on the collection, analysis, and monetization of user data to generate revenue, optimize services, and target customers. These models often provide free services in exchange for personal data.

Economic value

The measurable benefit or monetary worth derived from personal data in digital markets. This includes its role in driving personalization, advertising, and predictive analytics, which create competitive advantage and economic returns for platforms.

Market concentration

A market condition where a small number of firms hold a large market share, reducing competition. In digital markets, it results from platforms' control over data, infrastructures, and user bases, making entry for newcomers difficult.

Surveillance capitalism

A term coined by Shoshana Zuboff to describe a new economic system where companies profit from tracking, analyzing, and predicting user behavior by turning personal data into marketable commodities.

Nudging

A behavioral economics concept referring to subtle interventions designed to influence user decisions without restricting their choices. In digital platforms, nudging can guide user behavior toward certain actions (e.g., accepting terms or purchases) using interface design.

Political interference

The manipulation or influence of political processes through digital means, often via targeted advertisements or misinformation campaigns based on user data. The Cambridge Analytica case is a key example.

General Data Protection Regulation (GDPR)

A regulation enacted by the European Union in 2018 that sets comprehensive rules for data protection and privacy. It aims to give individuals greater control over their personal data through rights like consent, data portability, and the right to be forgotten.

Consent

A legal basis under the GDPR where individuals agree to the processing of their personal data. It must be freely given, specific, informed, and explicit for it to be valid under EU law.

Data portability

A GDPR right allowing individuals to obtain and reuse their personal data across different services. It promotes user autonomy by facilitating data transfer between platforms.

Right to be forgotten

A provision under GDPR that allows individuals to request the deletion of their personal data when it is no longer necessary for its original purpose, or when consent is withdrawn.

Data ownership

The concept that individuals should have full control and legal rights over their personal data, including how it is accessed, shared, or monetized. It contrasts with the current model, where platforms largely own and profit from user data.

Data dividends

A proposed economic model where users receive financial compensation for the data they generate and share with platforms, turning personal data into a source of individual income.

Data cooperatives

Collective structures where individuals pool their personal data and negotiate its access or use as a group. These aim to rebalance power toward users but face legal and organizational challenges.

International trade

The exchange of goods, services, and data across national borders. In the context of digital regulation, it refers to how differing privacy and data policies affect cross-border digital services and compliance.

Data localization policies

Government regulations requiring companies to store and process data within a country's borders. These policies are intended to protect data sovereignty and enhance security but may hinder international operations.

Privacy-enhancing technologies

Technological solutions designed to minimize personal data collection, enhance user anonymity, or allow data processing without exposing sensitive information. Examples include encryption and differential privacy.

Blockchain-based identity tools

Decentralized identity solutions that use blockchain technology to give users more control over their digital identities. They offer tamper-proof, verifiable identity records without relying on centralized authorities.

Decentralized data governance systems

Systems where the control over data access and usage is distributed across multiple actors rather than centralized platforms. These systems aim to increase transparency and user control.

Self-preferencing

A practice where platforms prioritize their own products or services over those of competitors within their ecosystem (e.g., showing their own apps higher in search results). This raises concerns about fairness and competition.

Mergers and acquisitions

Business strategies where a company buys or merges with another company to expand market share, eliminate competition, or integrate services. In digital markets, they are often used by dominant firms to reinforce their power.

Data-driven economies of scale

The economic advantage platforms gain by collecting and analyzing increasing volumes of data. The more data they gather, the more they can optimize operations and services, reducing marginal costs and increasing efficiency.

Behavioral profiling

The process of analyzing users' online actions uch as clicks, searches, and time spent on pages to create detailed profiles that predict preferences, interests, or future behavior.

Tracking

The systematic collection of user data across websites, devices, or applications to monitor online behavior. It enables targeted advertising, personalization, and data monetization.

Cambridge Analytica

A now-defunct data analytics firm involved in a major scandal for using Facebook user data without consent to influence political campaigns, most notably during the 2016 U.S. presidential election and the Brexit referendum.

Regulatory arbitrage

The practice of exploiting differences in regulations between jurisdictions, allowing companies to choose the most lenient or favorable legal environment to operate or process data.

Technological autonomy

The capacity of a region or country to develop, maintain, and control its own digital infrastructure, services, and innovations independently from foreign technology providers.

Neutral intermediaries

A status claimed by many digital platforms suggesting that they merely host or facilitate interactions (e.g., content sharing, transactions) without influencing or being responsible for the outcomes. This framing often exempts them from liability or regulatory obligations.

Market fairness

A principle in economic regulation ensuring that all actors, especially smaller or new entrants compete under equal and just conditions without undue advantage held by dominant firms.

Consumer rights

Legal entitlements that protect individuals in their interactions with businesses, including rights to privacy, transparency, consent, redress, and data control in the digital economy.

Contestability

An economic condition in which a market remains open and accessible to new entrants, even in the presence of dominant firms. A contestable market is characterised by low barriers to entry and exit, ensuring that competition is maintained not just by existing rivals but by the credible threat of potential competition.

Non-public data

Information generated through business or user interactions that is not accessible to the public. On digital platforms, this includes internal metrics, usage patterns, or transactional data that can provide strategic advantages if misused or withheld from competitors.

Device functionalities

Technical capabilities of a device (such as a smartphone or tablet) that allow applications or services to access features like geolocation, camera, contact lists, or biometric data. Under the DMA, gatekeepers must not restrict fair access to these functionalities for third-party services.

Self-preferencing

A practice where a platform unfairly favours its own products or services within its ecosystem, such as ranking them higher in search results or limiting the visibility of competing offers. This behaviour distorts competition and is explicitly prohibited under the DMA for gatekeepers.

Ex ante obligations

Legal duties or restrictions imposed proactively, before any harm has occurred. These obligations aim to prevent anti-competitive behaviours in advance, contrasting with ex post approaches that intervene only after an abuse is identified.

Article 102 TFEU

A provision of the Treaty on the Functioning of the European Union that prohibits firms from abusing a dominant position within the internal market if such conduct affects trade between Member States. It serves as a traditional legal basis for antitrust enforcement in the EU.

Architecture

In the digital context, architecture refers to the structural design of platforms, including how features, data flows, and user interfaces are organised. It plays a key role in shaping user behaviour and determining how power and control are distributed within a platform ecosystem.

Friction

Design elements or processes that slow down or complicate user actions. In platform regulation, friction can be used strategically to steer user behaviour, such as making it harder to opt out of tracking or switch services, thereby reducing user autonomy.

Information control

The ability of a platform to decide what information is accessible, how it is presented, and to whom. This includes control over user data, content visibility, and algorithmic filtering, giving dominant platforms significant influence over market dynamics and user decisions.

Neutralise

In a regulatory context, this means to reduce or eliminate the negative impact of certain platform behaviours or advantages. The DMA seeks to neutralise the structural power of gatekeepers by imposing obligations that prevent unfair market shaping.

Artificial intelligence features

Functionalities integrated into digital platforms that rely on machine learning or other AI techniques to deliver personalised or automated services. In apps like WhatsApp, this includes features such as automated message classification, content suggestions, or predictive actions.

User autonomy

The degree to which users have control over their digital environment, including decisions about data sharing, service usage, and content interaction. The DMA aims to reinforce user autonomy by ensuring transparency, consent, and the ability to choose alternative services.

Data separation

A regulatory requirement under the DMA that obliges gatekeepers to keep data collected across different services functionally separate. This prevents platforms from combining user data across services in ways that might reinforce dominance or undermine privacy.

Messaging services

Digital communication platforms that enable the exchange of messages between users, such as WhatsApp, Messenger, or iMessage. Under the DMA, gatekeepers operating messaging services are required to ensure interoperability with competing services upon request to promote user choice and reduce lock-in.

Switching costs

The financial, technical, or psychological costs a user incurs when changing from one service or platform to another. High switching costs discourage competition by making it difficult for users to leave dominant platforms, thereby reinforcing market concentration.

Multi homing

The practice of using several competing platforms or services simultaneously. Encouraging multi homing reduces user dependency on a single provider and is seen as a way to foster competitive pressure in digital markets.

Business users

Companies or professionals that use digital platforms to reach consumers or offer products and services. In the DMA, business users are granted specific rights to ensure fair access to data and communication tools controlled by gatekeepers.

User interaction data

Information generated through users' engagement with a service, such as clicks, search queries, purchases, or session duration. The DMA requires gatekeepers to share such data with the business users who generate it to reduce asymmetries.

Non-discriminatory access

A principle ensuring that all actors are treated equally and fairly by the platform, especially in terms of access to tools, algorithms, or ranking systems. The DMA obliges gatekeepers to provide fair conditions to avoid self-preferencing or hidden advantages.

Enforcement

The process of ensuring that legal or regulatory obligations are effectively applied and respected. In the DMA context, enforcement includes monitoring compliance, investigating violations, and applying sanctions when necessary.

Platform functionalities

Core features provided by a digital platform that enable third-party services to run or integrate, such as payment processing, authentication, push notifications, or access to sensors and APIs. Under the DMA, gatekeepers must not restrict fair access to these functionalities for other service providers.

Small and medium-sized firms

Businesses with limited staff or turnover, commonly defined in the EU as having fewer than 250 employees and less than €50 million in turnover. In the DMA context, these firms are seen as potential beneficiaries of reduced entry barriers and fairer competition conditions.

User base

The total number of individuals actively using a digital service or platform. A large user base gives platforms strategic advantages, including more data collection, stronger network effects, and higher attractiveness for advertisers or third-party developers.

Data flows

The movement and exchange of data within and across digital services or infrastructures. In regulatory contexts, controlling or opening up data flows is critical to ensuring competition, interoperability, and data protection compliance.

Encryption

A method of securing data by converting it into an unreadable format that can only be decoded with a specific key. Encryption is essential to maintaining the privacy and integrity of communications, particularly in messaging services subject to interoperability obligations.

Portability

The ability of users to retrieve and transfer their personal data from one digital service to another in a structured, commonly used, and machine-readable format. This right is reinforced in both the GDPR and the DMA to enhance user autonomy and platform competition.

Personalised content

Digital information tailored to individual users based on their preferences, behaviour, or demographic data. While it can improve user experience, personalisation also raises concerns around data exploitation, privacy, and algorithmic bias.

Innovation ecosystems

Interconnected networks of firms, institutions, technologies, and users that collaboratively drive innovation within a particular domain or region. The DMA aims to rebalance these ecosystems by limiting the control that dominant platforms have over access, data, and visibility.

Revitalise

In the context of policy and regulation, to inject new dynamism into a market or system. Scholars argue that the DMA could revitalise digital innovation by opening up previously inaccessible market segments.

Regulatory consistency

The degree to which rules and enforcement are applied uniformly across different jurisdictions. Lack of consistency can create uncertainty for firms and reduce the effectiveness of EU-level regulation like the DMA.

Extraterritorial enforcement

The application or influence of a regulation beyond the borders of the regulating authority. The DMA may lead non-European firms to adjust their global practices to meet EU standards, a dynamic often referred to as part of the Brussels effect.

Lawfulness, fairness, transparency

Three core principles of data protection under the GDPR.

Lawfulness means that data processing must have a valid legal basis.

Fairness implies that data must not be used in ways that are unjust or misleading to the individual.

Transparency requires that individuals are clearly informed about how their data is used.

Data minimization

A principle under the GDPR stating that only the minimum necessary personal data should be collected for a given purpose. This reduces the risks of misuse and enhances user privacy.

Purpose limitation

The idea that personal data must only be collected for specific, explicit, and legitimate purposes, and not further processed in a way incompatible with those purposes.

Principle of proportionality

A legal and ethical concept requiring that data processing activities be limited to what is strictly necessary to achieve a clearly defined and legitimate purpose. It helps ensure that user data is not used excessively or arbitrarily.

Sensitive data

Types of personal data considered more private and requiring higher protection, such as information about health, race, religion, sexual orientation, or biometric identifiers. Under the GDPR, processing sensitive data is generally prohibited unless specific legal conditions are met.

User rights

A set of rights granted to individuals under the GDPR, including access to data, rectification, erasure, data portability, and objection. These rights aim to give individuals more control over their personal information.

Rectification

The right of individuals to have inaccurate personal data corrected without undue delay.

Erasure

Also known as the "right to be forgotten", it allows individuals to request the deletion of their personal data under certain conditions.

Objection

The right of individuals to oppose the processing of their personal data, particularly in cases involving direct marketing, public interest, or legitimate interest by the data controller.

Privacy by design and by default

A principle requiring that data protection measures be integrated into systems and business practices from the start (by design), and that only data necessary for each specific purpose is processed by default.

Data Protection Impact Assessments (DPIAs)

A formal process required under the GDPR for evaluating and mitigating privacy risks of data processing activities, especially those that may pose a high risk to individuals' rights.

Data Protection Officer (DPO)

An independent expert responsible for overseeing data protection compliance within an organisation. DPOs are mandatory under the GDPR in certain cases, such as when processing large-scale sensitive data.

Accountability

A key GDPR principle requiring that organisations not only comply with data protection obligations but also be able to demonstrate their compliance through documentation, audits, and other means.

GDPR-CARPA

A voluntary certification mechanism under Article 42 of the GDPR, launched in Luxembourg. It allows organisations to demonstrate their compliance with data protection requirements via third-party audits, aiming to increase transparency and user trust.

Data governance

The framework of rules, processes, and responsibilities that guide how data is collected, managed, used, and protected within an organisation. Strong data governance ensures accountability, security, and compliance in handling personal data.

Compliance-by-design

An approach where regulatory and legal compliance is integrated from the beginning into product and service design, rather than being added as an afterthought. It ensures that privacy and data protection are embedded into the system architecture.

Corporate social responsibility (CSR)

A business philosophy where companies voluntarily integrate social and environmental concerns into their operations. In the context of GDPR, CSR can include responsible data use and the protection of user privacy.

Small and medium-sized enterprises (SMEs)

Businesses with limited resources and staff (fewer than 250 employees and a turnover of under €50 million). SMEs often face greater challenges in meeting GDPR compliance requirements due to cost and complexity.

Compliance-driven innovation

The creation or modification of products, services, or business models in response to regulatory requirements. Under GDPR, this can involve privacy-focused redesigns or the development of new tools that align with legal standards.

Privacy-enhancing technologies

Technological tools designed to protect personal data by reducing the amount of data collected, ensuring anonymity, or enabling secure processing. Examples include encryption, differential privacy, and secure multi-party computation.

Differential privacy

A method of data anonymization that adds random noise to datasets, allowing statistical analysis while protecting the privacy of individuals. It enables organisations to learn from data without exposing sensitive personal information.

Porter Hypothesis

An economic theory suggesting that well-crafted regulation can stimulate innovation and improve firm performance by encouraging companies to find efficient, socially aligned solutions.

Telecommunications and ICT sectors

Industries involved in the transmission of information (telecoms) and in the creation, processing, and storage of digital data (Information and Communication Technologies). These sectors are particularly impacted by data protection and privacy regulations like the GDPR.

Consent management

Processes and technologies that enable organisations to request, collect, track, and manage user consent for data processing. Consent must meet GDPR criteria to be valid freely given, specific, informed, and unambiguous.

Dark patterns

Design choices in digital interfaces that intentionally mislead or coerce users into taking actions they might not otherwise choose, such as accepting tracking or subscriptions. These patterns undermine informed consent and user autonomy.

Regulatory enforcement

The implementation and monitoring of legal rules by public authorities to ensure compliance. In the GDPR context, it refers to the capacity and actions of national and EU-level data protection authorities.

Data Protection Authorities (DPAs)

Independent public bodies established in each EU Member State responsible for monitoring and enforcing data protection laws, including the GDPR. Their effectiveness varies across countries depending on resources and capacity.

Irish Data Protection Commission (DPC)

The national DPA of Ireland, which plays a key role in GDPR enforcement due to the location of many tech companies' European headquarters in Ireland. It has faced criticism for slow decision-making and limited transparency.

Institutional implementation

How a regulation is applied and enforced through institutions, including the legal, administrative, and financial structures that support its functioning. Uneven institutional implementation can weaken the effectiveness of laws like the GDPR.

Data subjects

Individuals whose personal data is collected, held, or processed by an organisation. Under the GDPR, data subjects have rights such as access, rectification, and erasure.

Accountability

A principle under both the GDPR and the DMA requiring organisations to implement internal procedures and demonstrate that they comply with legal obligations, not merely in theory but through verifiable actions.

Business users

Firms or professionals that rely on digital platforms (such as marketplaces or app stores) to reach consumers. They depend on visibility, data access, and fair conditions to compete effectively.

Information asymmetry

A situation where one party (often a platform) possesses more or better information than the other (e.g., business users or consumers), creating power imbalances in decision-making and market interactions.

Data portability

A right under the GDPR that allows individuals to obtain and reuse their personal data across different services. It enhances user control and competition by lowering switching costs.

User empowerment

A concept that refers to enhancing individuals' control over their digital experiences, particularly their data, choices, and platform interactions. It is promoted through rights like portability and transparency.

Explicit consent

A clear and affirmative agreement given by a user to allow the processing of their personal data for a specific purpose. Under GDPR, it must be freely given, informed, and specific.

Purpose limitation

A data protection principle stating that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

User privacy

The right of individuals to control how their personal data is collected, used, and shared. It is central to the GDPR and is often balanced against other goals such as interoperability or innovation.

Legal basis

A justification under the GDPR that allows for the lawful processing of personal data. Examples include user consent, contractual necessity, legal obligations, or legitimate interest.

Data controller

An entity (individual or organization) that determines the purposes and means of processing personal data. The controller bears responsibility for ensuring GDPR compliance.

Erasure

Also known as the "right to be forgotten", it allows individuals to request the deletion of their personal data when it is no longer necessary or when consent is withdrawn.

Federated learning

A machine learning technique where an algorithm is trained across multiple decentralized devices or servers holding local data, without transferring the data itself. It helps preserve privacy by keeping data localized.

Homomorphic encryption

An advanced cryptographic method that allows computation on encrypted data without decrypting it. It enables secure data processing while maintaining confidentiality.

Differential privacy

A privacy-enhancing technique that adds statistical noise to data, ensuring that individual-level information cannot be inferred from aggregate datasets. It balances utility and privacy in data analysis.

Data sharing

The process of making personal or non-personal data available to other entities (e.g., platforms, service providers) for specific purposes. In the context of the DMA, it is often mandated to improve interoperability.

Pseudonymisation

A data protection technique where personal identifiers are replaced with pseudonyms or codes. While it reduces the risk of identification, it does not make the data fully anonymous and is still considered personal data under the GDPR.

Regulatory obligations

Legally binding duties imposed on companies or entities by regulatory frameworks such as the GDPR or DMA. These obligations define what is permissible, required, or prohibited in terms of data processing, transparency, or fair competition.

Long-term theoretical framework

A conceptual model used to anticipate and analyze the evolution of legal and regulatory systems over time. In the context of the DMA and GDPR, it refers to structured thinking about how these frameworks will interact in the future.

Integrated governance

A coordinated regulatory approach that ensures consistency and coherence between different legal instruments and enforcement bodies. It often involves collaboration between EU institutions and national regulators.

Digital Services Act (DSA)

A 2022 European regulation that complements the DMA by focusing on the responsibilities of digital platforms regarding content moderation, algorithmic transparency, and user safety in the online environment.

AI Act

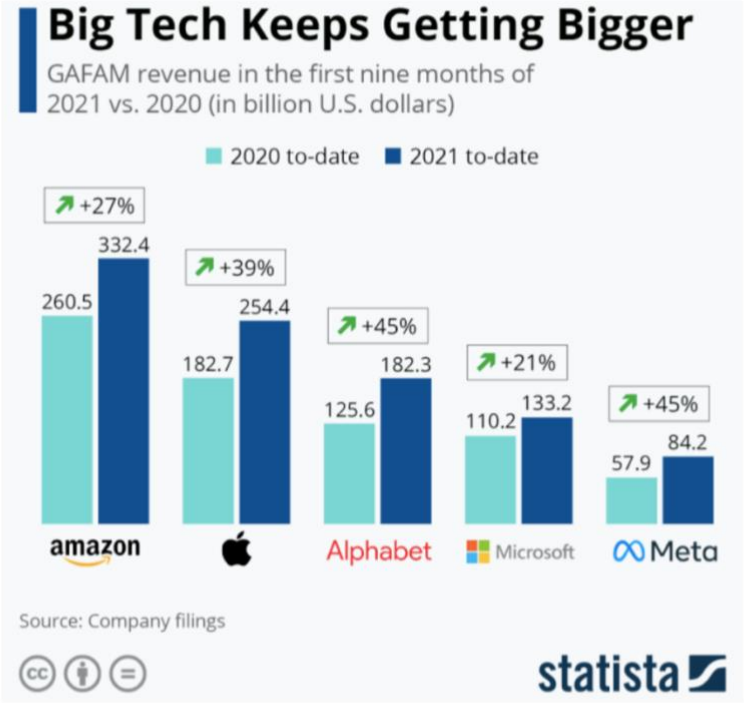
A forthcoming EU regulation aiming to establish a legal framework for artificial intelligence. It categorizes AI systems based on risk and imposes strict requirements on high-risk applications to ensure safety, transparency, and fundamental rights compliance.

SaaS (Software as a Service)

A cloud-based software delivery model in which applications are accessed online via subscription, rather than installed locally. SaaS solutions are centrally hosted by providers and delivered over the internet, enabling real-time updates, cost efficiency, and scalability. In the European digital ecosystem, SaaS is particularly relevant for SMEs and B2B platforms, and raises key issues under the GDPR (data processing responsibilities, cross-border data flows) and the DMA (platform dependence, interoperability, and switching costs). Examples include CRM tools like Salesforce, collaborative platforms like Google Workspace, and accounting systems like Odoo.

Appendix B: Charts, Figures and Visual Data

Figure B.1. : Chart illustrating the revenue growth of GAFAM companies between 2020 and the first nine months of 2021 (in billions of US dollars)



Zandt F. (2021, 29 octobre). *Big Tech keeps getting bigger*, Statista, https://www.statista.com/chart/21584/gafam-revenue-growth/

This figure highlights the significant increase in revenue among major tech firms (Google, Apple, Facebook, Amazon, Microsoft) over the 2020–2021 period, reflecting their dominant position in global digital markets. Such growth reinforces the relevance of regulatory scrutiny under the DMA, especially regarding market concentration and platform gatekeeping practices.

Figure B.2. : Digital privacy ontology: how personal data is processed, managed and monetised in the digital economy

This figure illustrates the transformation of personal data from a privacy concern into a managed asset that fuels platform strategies, predictive analytics, and personalised services. It reflects how data flows are governed by both user interaction and technical systems, shaping the foundation of data-driven business models in the digital economy.

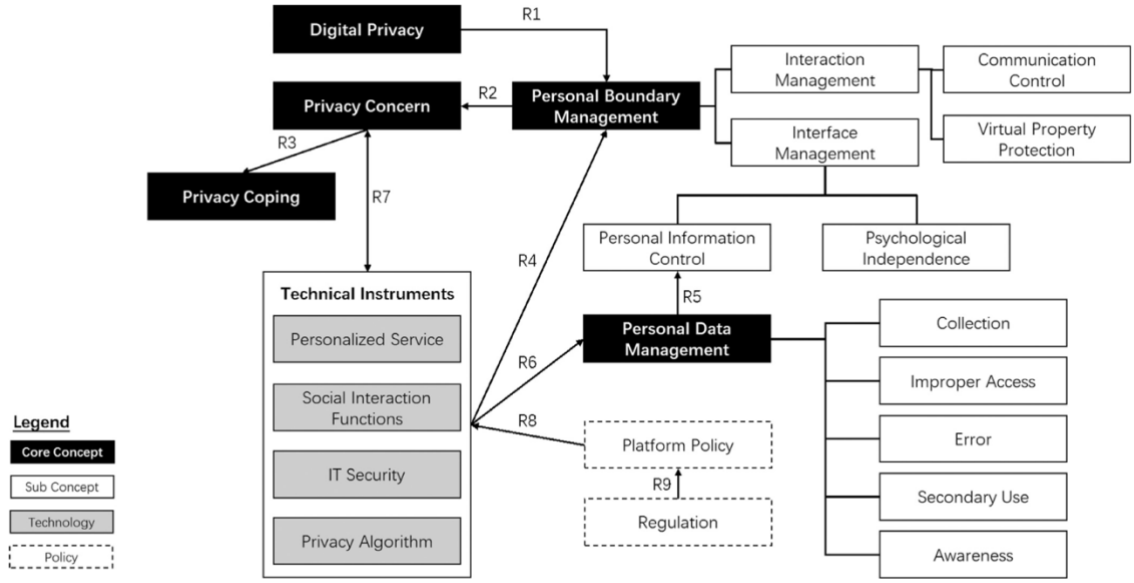


Fig. 1. Digital privacy ontology.

Wang, Y. D., Zhang, Y., & Wang, H. (2021). Exploring the ontology of digital privacy: A data-centric perspective. *Information Systems Frontiers*, 23(3), 543–562. https://doi.org/10.1007/s10796-020-10004-2

Figure B.3. : Evolution of media advertising market in Europe (2009–2015)

Table 1: Evolution of media advertising market in Europe (PricewaterhouseCoopers, 2014)

	2009	2010	2011	2012	2013	2014	2015
TV	21.239	23.034	23.164	21.989	21.531	22.004	22.542
Radio	4.345	4.498	4.494	4.397	4.389	4.434	4.503
Newspapers	18.065	17.753	17.245	15.875	15.064	14.453	13.903
Magazines	8.291	8.445	8.383	7.824	7.672	7.596	7.520
Online	13.606	15.795	18.376	20.762	23.545	26.130	28.549

Evans, D. S. (2018). *Attention platforms, the value of user data, and regulatory implications*. SSRN. https://doi.org/10.2139/ssrn.3044858

Figure B.4. : Overview of GDPR Opening Clauses Allowing National Flexibility

These tables list the main "opening clauses" of the General Data Protection Regulation (GDPR), which allow EU Member States to introduce specific national rules on key provisions such as lawful processing, children's consent, sensitive data, and the designation of Data Protection Officers. These clauses illustrate the potential divergence in implementation, even within a harmonised European legal framework.

Table 8.1 Opening clauses under the GDPR

Provision of the GDPR	Subject matter	Content of the opening clause
Art. 4 No. 7	Definition of 'controller'	Where the purposes and means of certain processing activities are determined by EU Member State law, the controller or the specific criteria for its nomination may be provided for by EU Member State law.
Art. 6 Sec. 2	Lawfulness of processing	EU Member States may maintain or introduce more specific provisions regarding the lawfulness of (i) processing based on a legal obligation of the controller or of (ii) processing carried out in the public interest by determining more precisely specific requirements for such processing and other measures to ensure lawful and fair processing (Sect. 4.2.2.3).
Art. 8 Sec. 1	Conditions applicable to child's consent in relation to information society services	EU Member State law may provide for a *lower minimum age for a valid child's consent* provided that it is not below 13 years (Sect. 4.2.1.6).
Art. 9 Sec. 2	Processing of special categories of personal data	EU Member States may provide for different deviating provisions in this regard, such as to *exclude processing of sensitive personal data based on* the data subject's *consent* or rules regarding processing in the employment context, etc. (Sect. 4.2.3).
Art. 9 Sec. 4	Processing of special categories of personal data	EU Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health (Sect. 4.2.3).
Art. 10	Processing of personal data relating to criminal convictions and offences	Processing of personal data relating to criminal convictions and offences may be carried out when it is authorised by EU Member State law (Sect. 4.2.3.3).
Art. 14 Sec. 5 lits. c–d	Information to be provided where personal data has not been obtained from the data subject	The *information obligation* of the controller *does not arise* if the obtainment or disclosure of personal data is expressly laid down by EU Member State law or where the personal data must remain confidential subject to an obligation of professional secrecy regulated EU Member State law (Sect. 5.2.3).

(continued)

Table 8.1 (continued)

Provision of the GDPR	Subject matter	Content of the opening clause
Art. 17 Sec. 1 lit. e; Sec. 3 lit. b	Right to erasure	The controller is *obliged to erase* personal data based on a legal obligation in EU Member State law to which it is subject. As counterpart for such erasure obligation, however, a right to erasure does *not arise if processing is required* for compliance with a *legal obligation* under EU Member State law (Sect. 5.5.2).
Art. 22 Sec. 2 lit. b	Automated individual decision-making	The *general prohibition* of automated decision-making does *not* apply *where* the latter *has been authorised* by EU Member State law to which the controller is subject (Sect. 5.8).
Art. 23	Restrictions	EU Member State law may *restrict the scope of the data subject rights* and corresponding obligations of data processing entities for various public-interest-related reasons (Sect. 5.9).
Art. 26	Joint controllers	EU Member State law may determine the respective data protection obligations of joint controllers.
Art. 28 Sec. 3 lits. a, g; Sec. 4	Processor	EU Member State law may – permit processors to carry out processing without authorisation of the controller; – require them not to delete personal data after the termination of their services for the controller; – lay down rules on the involvement of sub-processors.
Arts. 32 Sec. 4	Security of processing	EU Member State law may require individuals acting under the authority of a controller/processor to process personal data even though they have not been instructed to do so by said controller/processor.
Art. 35 Sec. 10	Data Protection Impact Assessment	A Data Protection Impact Assessment will not be required where processing is based on EU Member State law introduced under Art. 6 Sec. 2 GDPR and a general impact assessment has already been carried out in the context of the adoption of that legal basis (Sect. 3.5).

(continued)

Table 8.1 (continued)

Provision of the GDPR	Subject matter	Content of the opening clause
Art. 36 Sec. 5	Prior consultation	EU Member State law may require controllers to consult with, and obtain prior authorisation from, the Supervisory Authority in relation to its processing activities carried out for the performance of a task in the public interest.
Art. 37 Sec. 4	Designation of the data protection officer	EU Member State law may *introduce further obligations* for controllers/processors *to designate a DPO* (Sect. 3.6).
Art. 39 Sec. 1 lits. a, b	Tasks of the data protection officer	The DPO shall inform and advise the data processing entities on data protection obligations pursuant to EU Member State law and monitor compliance with such provisions (Sect. 3.6).
Art. 49 Sec. 1 lit. d, g; Secs. 4, 5	Derogations for specific situations	A third-country data transfer may be lawful based on public interests recognised by EU Member State law or if it is made from a register intended to provide information to the public according to EU Member State law. EU Member State law may limit third-country transfers of sensitive data for reasons of public interest (Sect. 4.3.7).
Art. 58 Sec. 1 lit. f; Sec. 6	Powers	On-site inspections by the Supervisory Authorities must be carried out in accordance with EU Member State law. Each EU Member State may grant its Supervisory Authority additional powers by law (Sect. 7.1).
Art. 84 Sec. 1	Penalties	EU Member States shall lay down *rules on other penalties for infringements* of the GDPR, in particular when the latter are not subject to administrative fines (Sect. 7.3).

involved.[1] These clauses *either allow* EU Member States, pursuant to the specific terms of each provision, *to replace, complement or further specify the provisions* of the GDPR.[2]

[1] Laue, ZD 2016, 463, 464; Laue/Nink/Kremer, Datenschutzrecht, Einführung (2016), rec. 113.
[2] Laue, ZD 2016, 463, 464.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Cham: Springer. pp. 220–222.

Figure B.5. : Overview of Interview Requests and Respondent Status

	Target Profile	**Resaon for selection**	**Interview status**	**Duration**	**Notes**	**Related section**
1.	EU Official (anonymized)	Regulatory perspective on GDPR enforcement and institutional views	Conducted	51 minutes	Confirmed use of centent	Part 4.2. regulatory context
2.	Tech journalist at Euractiv	Expert media insights on EU regulation debates and DMA evolution	Contact made, pending		Out of office response received	Part 4.2. regulatory context
3.	Professor of European Law (UCL)	Academic perspective on the legal interpretation of GDPR and DMA	Conducted	42 minutes	Anonymous upon request	Part 4.2. regulatory context
4.	Professor in innovation strategy (anonymized)	Insights on business models and innocation under regulation	Conducted	43 minutes	Quotes used with approval	Part 4.3. business and innovation impacts
5.	Security manager at Elium (knowledge management plateform)	Practical view on GDPR and DMA impact on tech firm	Conducted	37 minutes		Part 4.3. business and innovation impacts

6.	Representative from Mistral AI	Start-up perspective on AI development in a regulated environment	No response		Contact attempt unsuccessfull	Part 4.3 .business and impacts
7.	Representative from Odoo (Belgian software company)	SME insight into compliance with GDPR and platform regulations	No response		Contact attempt unsuccessfull	Part 4.3 .business and impacts
8.	Representative from Google	Platform gatekeeper perspective under DMA obligations	No response		Contact attempt unsuccessfull	Part 4.3 .business and impacts
9.	Representative from BEUC (European consumer organization)	Consumer rights viewpoint on data protection and platform power	Declined		Too busy to particpate	Part 4.3 .business and impacts
10.	Representative from Test-Achat (Belgian consumer association)	National consumer perspective on digital regulation impact	No response		Contact attempt unsuccessfull	Part 4.3 .business and impacts

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Cham: Springer. pp. 220–222.

Figure B.6. : Illustrative Cases of Digital Harms in the Absence of Regulation

This table presents selected examples of digital harms caused by major platforms in the absence of appropriate regulatory frameworks. It highlights risks such as privacy violations, competitive distortion, surveillance practices, and the spread of disinformation risks that the GDPR and DMA aim to mitigate.

Illustrative Cases of Digital Harms in the Absence of Regulation

Platform	Type of Risk	Description	Regulation Previously Absent
WhatsApp/Meta	Privacy	Integration of user data without meaningful consent	GDPR
Meta Platforms	Competitive Advantage	Cross-service data pooling reinforcing gatekeeper position	GDPR and DMA
TikTok	Privacy and Surveillance	Biometric tracking and weak protections for minors	GDPR
Facebook	Disinformation	Algorithmic promotion of misleading content without transparency	No horizontal governance

Source: Author's own compilation based on interviews and regulatory analysis (2025).

Figure B.7. : Comparative Table - Compliance Strategies and Competitive Impact Across Digital Firms

This comparative table outlines how different categories of digital firms such as large foreign platforms, European start-ups, and mid-size EU SaaS companies approach regulatory compliance under the GDPR and DMA. It highlights strategic adaptations, operational challenges, and the perceived effects on competitiveness in the European digital market.

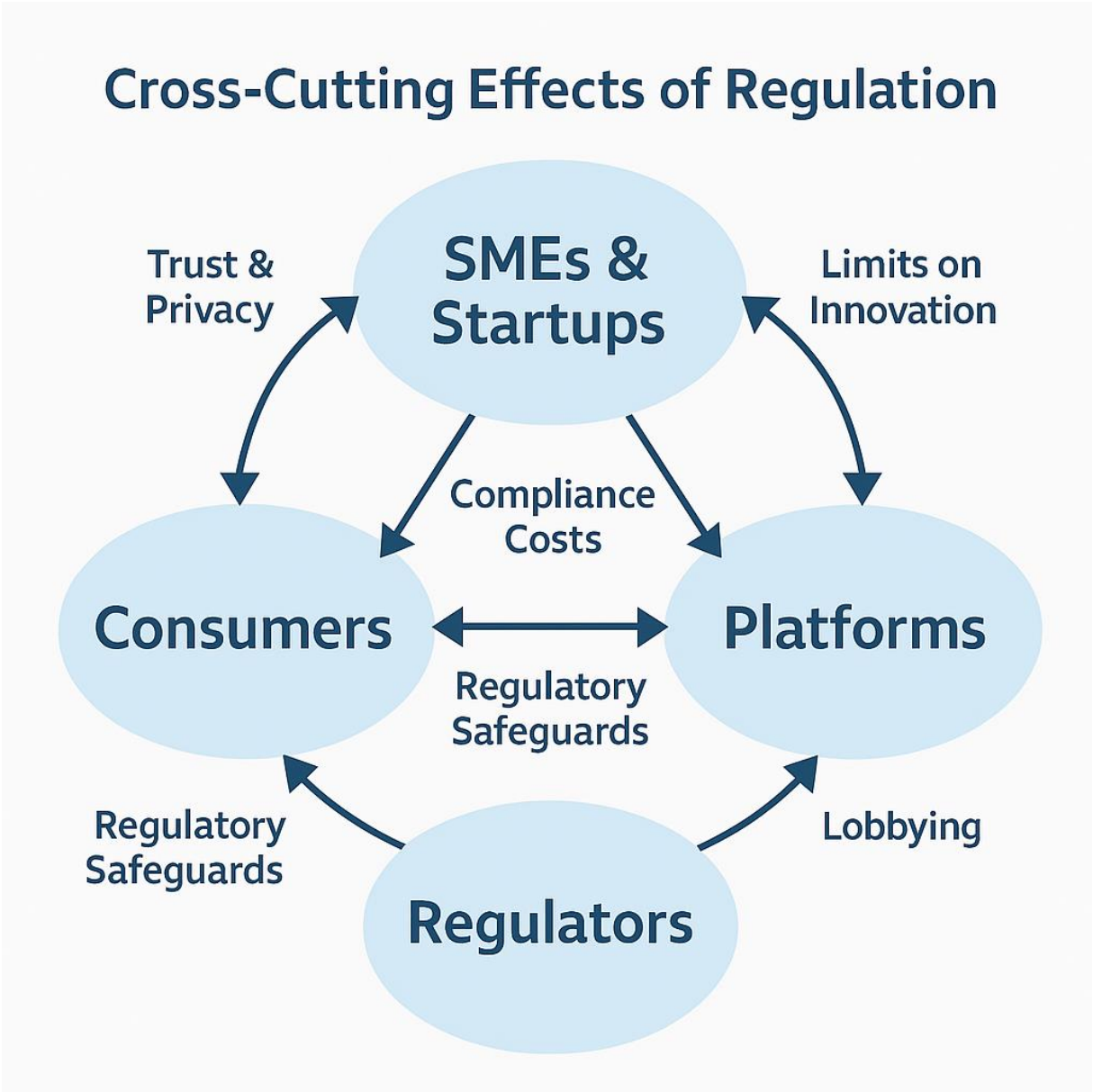
Comparative Table: Compliance And Competitive Impact

	Type of Actor	Compliance Strategy	Main Challenges	Perceived Competitive
1	Large foreign platforms (e.g. Meta, Google)	Influence regulation through lobbying; adapt minimally to maintain market access	Maintaining market share while complying with stricter rules; adapting global	Moderate, due to scale and ability to absorb compliance costs
2	European start-ups (e.g. Elium)	Integrate GDPR compliance from design stage (privacy by design); adapt technical	Resource-intensive compliance process; slower scaling due to technical and	Significant short-term burden but potential for long-term trust-based
3	Mid-size EU SaaS companies	Enhance compliance to differentiate on data security, transparency, and	Managing subcontractors, anticipating client-specific legal clauses,	Mixed: compliance as both commercial lever and operational complexity

Source: Author's own elaboration based on expert interviews and regulatory literature (2025).

Figure B.8. : Cross-Cutting Effects of GDPR and DMA on Key Stakeholders

This diagram illustrates the primary interactions and regulatory effects of the GDPR and the DMA on the main stakeholder groups: consumers, small and medium-sized enterprises (SMEs), large digital platforms, and regulators. While consumers benefit from increased transparency and control over their data, SMEs face significant compliance costs but may also gain credibility. Large platforms encounter restrictions on market behavior and data integration, while regulators navigate enforcement challenges and geopolitical influence. The arrows reflect the reciprocal nature of these pressures across the ecosystem.



Source: Author's own elaboration based on expert interviews and regulatory literature (2025).

Appendix C : Preparation of the Interviews

Appendix C.1. : Approach and interview questionnaire with an employee of the European Commission for the second part of the thesis

Pour cette interview avec EU offical l'objectif sera de comprendre, d'un point de vue opérationnel et juridique, comment la régulation des données personnelles (GDPR) s'articule face à des enjeux technologiques non encore totalement encadrés, en particulier dans les scénarios sans régulation claire.

Ce questionnaire visera donc à :

- explorer les limites actuelles de la régulation dans un environnement numérique évolutif,
- identifier la capacité réelle des autorités de protection à agir dans des contextes transfrontaliers et face à des acteurs puissants,
- et réfléchir à l'articulation potentielle entre régulation publique et approches alternatives (co-régulation, soft law, standards techniques, etc.).

Questionnaire pour entretien avec EU offical – Thématique : données personnelles, limites du cadre actuel, scénarios sans régulation

Introduction avec rappel contextuel

Contexte de l'entretien : Dans le cadre de mon mémoire de fin d'études à la Louvain School of Management, j'analyse les effets combinés du Digital Markets Act (DMA) et du General Data Protection Regulation (GDPR) sur les marchés numériques européens. Ma recherche s'inscrit dans une perspective multidimensionnelle (technologie, droit, stratégie), et vise notamment à comprendre comment les entreprises réagissent en l'absence ou en complément de régulations claires.

Le GDPR, pilier de la régulation européenne des données, vise à renforcer les droits des individus et impose aux entreprises un cadre strict de traitement et de gouvernance des données. Mais dans un contexte de forte innovation technologique (IA, tracking, cloud, etc.) et de jeux transfrontaliers, certaines zones grises persistent.

Cet entretien, dans le cadre de la partie 2 de mon mémoire, vise à explorer ces “zones sans régulation explicite” et à comprendre le rôle effectif et stratégique de l’EDPB dans un tel contexte.

I. Gouvernance des données dans un monde numérique en mouvement

1. Comment décririez-vous les principaux défis pour l’application effective du GDPR dans un environnement technologique aussi dynamique que celui des plateformes numériques ?
2. Selon vous, quelles sont aujourd’hui les limites concrètes du GDPR face à des pratiques émergentes comme l’entraînement d’IA génératives, la biométrie passive ou l’interopérabilité forcée ?
3. Le GDPR repose beaucoup sur les principes de "responsabilisation" et "accountability". Ces principes sont-ils suffisants en l’absence de régulation complémentaire (comme le DMA ou l’AI Act) ?

II. Capacité d’action du régulateur et coopération transfrontalière

4. L’EDPB dispose-t-il aujourd’hui des moyens humains et techniques suffisants pour répondre aux défis posés par des entreprises de dimension globale ?
5. Quels sont les freins institutionnels ou juridiques qui empêchent une application uniforme du GDPR au sein de l’UE ?
6. La fragmentation dans les décisions nationales (ex : DPC irlandais vs CNIL française) remet-elle en question l’efficacité du GDPR en tant que cadre européen unique ?

Data Protection Commission – Irlande
Commission nationale de l’informatique et des libertés – France
l'exemple « DPC irlandais vs CNIL française » fait référence aux différences d’approche ou de rigueur entre autorités nationales de protection des données, qui appliquent toutes le RGPD mais avec des interprétations ou des priorités parfois divergentes.

III. Scénarios sans régulation claire & rôle de l’EDPB

7. Dans des secteurs où la régulation est encore floue (comme l'IA générative ou les métavers), comment l'EDPB peut-il intervenir de manière proactive ?

8. Voyez-vous un rôle pour des mécanismes d'autorégulation ou de co-régulation dans la gouvernance des données à l'échelle européenne ?

9. Le recours à des standards techniques ou à des certifications (comme les codes de conduite ou GDPR-CARPA) pourrait-il devenir un levier plus important dans les prochaines années ? Sous quelles conditions ?

CARPA signifie Certified Assurance Report-based Processing Activities. C'est un mécanisme de certification développé par l'APD (l'Autorité de protection des données belge) dans le cadre du RGPD.
Plus simplement, GDPR-CARPA est un label de conformité RGPD délivré par un organisme indépendant accrédité. Il repose sur un audit formel et structuré, avec un rapport d'assurance, pour vérifier qu'une organisation traite les données personnelles de manière conforme au RGPD.

IV. Perspectives et évolutions du cadre réglementaire

10. Le GDPR est parfois perçu comme freinateur pour l'innovation, en particulier chez les start-ups. Partagez-vous ce constat ? Comment concilier innovation et protection ?

11. L'articulation entre le GDPR et d'autres régulations sectorielles (DMA, DSA, AI Act) est-elle aujourd'hui bien intégrée dans les travaux du Comité ? Quels risques de chevauchements ou conflits voyez-vous ?

12. À votre avis, quels ajustements seraient nécessaires pour renforcer l'efficacité du GDPR dans les années à venir, en particulier dans des contextes technologiques extrêmes ou non prévus initialement ?

Conclusion

13. En un mot, selon vous, quels sont les risques majeurs si l'Europe ne parvient pas à compléter ou adapter son arsenal réglementaire face aux évolutions numériques ?

14. Quel rôle voyez-vous pour l'EDPB dans le futur des marchés numériques : arbitre juridique, coordinateur technique, ou organe stratégique plus global ?

Appendix C.2. : Approach and interview questionnaire for the journalist at Euractiv for the second part of the thesis (in French and English)

Interview Questions (EN) – Digital Journalist (Euractiv) – Strategic and Political Perspectives on the GDPR and DMA

Introduction for the interview

I'm a Master's student at UCLouvain (Louvain School of Management) currently writing a thesis on the interaction between the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA), and their combined impact on business models and innovation strategies in Europe's digital markets. I would really appreciate your insight on the political, strategic, and narrative aspects of these two landmark regulations – as well as your perspective on what might have happened had they not been adopted.

I. Political and strategic framing

1. How would you describe the political narrative behind the GDPR and DMA? Were they mainly framed around user protection, rebalancing power with large platforms, or European digital sovereignty?
2. In your view, what were the main political forces or pressures that enabled these texts to move forward, despite opposition from certain member states or industry lobbying?
3. Do you think global tensions (with the US, China, or others) helped accelerate the EU's push to regulate Big Tech?

II. What if the EU had done nothing?

4. What risks or negative developments do you think might have occurred if the EU had not introduced the GDPR and DMA? For example, in terms of privacy, market dominance, manipulation, or transparency?

5. Are there examples from outside the EU (e.g. the US, India, or emerging markets) where a lack of regulation has led to significant digital imbalances or abuses?
6. As the DMA is still being implemented, what gaps or weak points have you already identified, or what do you see as possible future issues?

III. Regulation and innovation: a contradiction?

7. Many actors argue that too much regulation stifles innovation. Others say it creates a "slow Europe." What is your assessment of that tension?
8. Could strong regulation actually help build more resilient and ethical European tech companies in the long term?
9. Have you seen companies using their GDPR/DMA compliance as a strategic advantage – either in communications, marketing, or positioning?

IV. Media's role and the EU's global influence

10. What role can journalists like yourself play in clarifying these complex regulations – both for citizens and policymakers?
11. Do you feel the voice of citizens and consumers is sufficiently heard in the debates on digital regulation? Or is it often overshadowed by economic and institutional concerns?
12. The GDPR is often cited as a "Brussels effect." Do you think the DMA might follow a similar path in influencing global standards?

Conclusion

13. From your perspective, what are the next big priorities in EU digital regulation? For example, algorithmic transparency, data access, AI business models, etc.?
14. Finally, what advice would you give to a young researcher or student trying to better understand how digital policymaking works in Europe?

Appendix C.3. : Approach and interview questionnaire for the legal expert and professor of European law at UCL for the second part of the thesis – Alain Strowel

Questionnaire pour entretien avec un juriste en droit européen – Thématique : absence de régulation & autorégulation dans les marchés numériques

Introduction

Contexte de l'entretien : Je suis étudiant en Master à la Louvain School of Management, et je réalise un mémoire sur l'impact combiné du Digital Markets Act (DMA) et du General Data Protection Regulation (GDPR) sur les marchés numériques européens. Mon objectif est d'examiner dans quelle mesure ces deux régulations influencent les modèles économiques et les stratégies d'innovation des entreprises opérant dans l'UE.

Pour rappel :

- Le DMA, adopté en 2022, impose des obligations ex ante aux grandes plateformes numériques (dites "gatekeepers") afin de garantir la contestabilité des marchés et de limiter les pratiques anticoncurrentielles comme l'auto-préférencement ou le verrouillage de l'écosystème.
- Le GDPR, en vigueur depuis 2018, renforce les droits des utilisateurs sur leurs données personnelles et impose aux entreprises des obligations strictes de transparence, de minimisation et de sécurité dans le traitement des données.

Cet entretien s'inscrit dans la partie 2 de mon mémoire, qui analyse les risques liés à l'absence de régulation, ainsi que les scénarios alternatifs (notamment l'autorégulation). Je souhaiterais bénéficier de votre expertise en droit européen, et plus particulièrement sur les mécanismes juridiques d'autorégulation.

I. Cadre général et vision juridique

1. Selon vous, quels sont les risques principaux liés à l'absence de régulation publique dans les marchés numériques, notamment en matière de concurrence et de protection des données ?
2. Le modèle européen repose en partie sur une régulation ex ante (DMA) et des droits fondamentaux (GDPR). Quels seraient, selon vous, les impacts d'un modèle purement auto-régulé ?

3. Comment les principes du droit européen encadrent-ils ou limitent-ils les mécanismes d'autorégulation dans le secteur numérique ?

II. L'autorégulation comme solution juridique viable ?

4. L'autorégulation est-elle, selon vous, une alternative crédible au niveau européen pour encadrer les pratiques des grandes plateformes numériques ? À quelles conditions ?
5. Quelles différences faites-vous entre autorégulation, co-régulation, et soft law dans le contexte du droit européen ?
6. Existe-t-il des exemples (dans ou hors du numérique) où l'autorégulation s'est révélée efficace en Europe ? Quels enseignements en tirer ?

III. Application à la technologie et aux plateformes

7. Quels sont les enjeux juridiques associés à des pratiques comme l'interopérabilité technique, la publicité comportementale ou le profilage algorithmique dans un cadre sans régulation ?
8. Que dit le droit européen actuel sur la responsabilité des plateformes lorsqu'aucune régulation sectorielle n'existe ?
9. Pensez-vous que des plateformes comme TikTok ou Meta pourraient s'auto-réguler efficacement sans intervention publique ? Pourquoi (pas) ?

IV. Perspectives et cadre d'évolution

10. Le droit européen pourrait-il évoluer vers une reconnaissance formelle de mécanismes d'auto-régulation dans le domaine des données ou de la concurrence numérique ?
11. Dans un contexte post-DMA/GDPR, pensez-vous qu'un retour partiel à des logiques de co-régulation pourrait être envisagé ?
12. Quels garde-fous seraient juridiquement nécessaires pour rendre ce type de mécanismes (auto- ou co-régulés) compatibles avec les droits fondamentaux ?

Conclusion

13. Selon vous, dans quelle mesure l'autorégulation peut-elle (ou non) constituer une réponse suffisante aux enjeux actuels des marchés numériques européens ?
14. Si vous aviez un conseil à formuler aux institutions européennes en matière de gouvernance future du numérique, quel serait-il ?

Appendix C.4. : Approach and interview questionnaire for the professor in innovation for the third part of the thesis

Questionnaire – Professeur anonyme (UCL) – Régulations européennes et dynamiques d'innovation

Introduction pour le professeur (à adapter à l'oral ou à l'écrit)
Je réalise un mémoire de fin d'études à la Louvain School of Management sur l'interaction entre le Digital Markets Act (DMA) et le General Data Protection Regulation (GDPR), et leur impact sur les modèles économiques et la capacité d'innovation des entreprises numériques en Europe. Votre expertise sur les stratégies d'innovation est particulièrement précieuse pour comprendre comment les entreprises s'adaptent (ou non) dans ce contexte réglementaire.

I. Régulation et innovation : une tension ou une opportunité ?

1. Selon vous, dans quelle mesure les régulations européennes (DMA et GDPR) freinent-elles ou stimulent-elles l'innovation dans les entreprises européennes ?
2. Le concept de "compliance-driven innovation" est parfois évoqué : est-il crédible dans la pratique, ou reste-t-il une exception ?

Compliance-driven innovation » désigne une innovation qui naît de la nécessité de se conformer à une régulation. Plutôt que de freiner les entreprises, une réglementation comme le RGPD ou le DMA peut pousser celles-ci à repenser leurs produits, à innover de manière plus éthique ou à se différencier sur le marché grâce à leur conformité. C'est l'idée que la contrainte réglementaire peut devenir un levier stratégique.

3. Le principe de “privacy by design” imposé par le GDPR est-il perçu par les entreprises comme une opportunité d’innovation, ou comme une contrainte technique ?

Privacy by design signifie que la protection des données personnelles est intégrée dès la conception d’un produit, service ou système, et non ajoutée après coup. Cela implique de penser la confidentialité comme un élément central de l’architecture technique et organisationnelle : minimisation des données collectées, sécurité par défaut, contrôle donné à l’utilisateur, etc. C’est un principe clé du RGPD.

II. Modèles économiques et stratégies d’adaptation

4. Observez-vous des transformations de modèles économiques directement liées à l’entrée en vigueur du DMA ou du GDPR ?

5. Est-ce que certains secteurs ou types d’acteurs (ex. : open source, plateformes SaaS, start-ups IA…) s’adaptent mieux que d'autres ?

6. Le DMA peut-il, selon vous, inciter certains acteurs à ajuster leur stratégie de croissance ou leur architecture de services pour éviter la désignation comme gatekeeper ?

Gatekeeper (ou contrôleur d’accès) est un terme utilisé dans le Digital Markets Act (DMA) pour désigner une grande plateforme numérique qui détient une position dominante lui permettant de contrôler l’accès entre les entreprises utilisatrices et les consommateurs finaux.

III. Europe vs. reste du monde : un désavantage compétitif ?

7. Est-ce que vous avez identifié des cas où les entreprises européennes sont défavorisées dans leur capacité d’innovation par rapport à leurs concurrentes américaines ou asiatiques, à cause du cadre réglementaire plus strict ?

8. Le cumul des régulations (DMA, GDPR, DSA, AI act…) en Europe crée-t-il un environnement trop rigide pour certains types d’innovateurs ?

9. À l'inverse, pensez-vous que la réputation de l'Europe comme leader en régulation éthique peut devenir un avantage stratégique (fiabilité, confiance, exportabilité des standards) ?

IV. Logiques d'apprentissage stratégique dans un cadre contraint

10. Certains professeurs (dont mon promoteur) évoquent l'idée que "lancer un produit en Europe" dans un contexte très réglementé peut permettre à une entreprise de mieux s'exporter ensuite vers des régions plus souples. Cette stratégie d'apprentissage sous contrainte vous semble-t-elle pertinente ?
11. Quels arbitrages stratégiques voyez-vous dans le choix entre conformité maximale et agilité innovante pour une start-up ?
12. Peut-on imaginer que les régulations deviennent des leviers d'innovation collaborative entre entreprises (interopérabilité, standards ouverts, co-innovation) ?

Conclusion libre

13. Avez-vous en tête des exemples concrets d'entreprises qui ont su transformer ces contraintes réglementaires en leviers d'innovation ?
14. Enfin, quel conseil stratégique donneriez-vous à une PME numérique européenne qui souhaite innover tout en restant conforme aux exigences européennes ?

Appendix C.5. : Approach and interview questionnaire for Elium (a knowledge management start-up based in Louvain-la-Neuve) for the third part of the thesis

Questionnaire – Elium (Louvain-la-Neuve) – Régulation numérique, innovation et stratégie en contexte RGPD/DMA

Introduction pour l'entretien (oral ou écrit) :

Dans le cadre de mon mémoire de Master 2 à l'UCLouvain (Louvain School of Management), je m'intéresse aux effets conjoints du RGPD et du DMA sur les entreprises européennes du numérique. Je souhaite comprendre comment ces cadres influencent

concrètement les modèles économiques, les stratégies d'innovation et les arbitrages réglementaires, notamment pour les start-ups technologiques actives dans des domaines comme la gestion de la connaissance, l'IA ou le SaaS collaboratif.

I. Conformité et gouvernance des données

1. Le RGPD a-t-il modifié votre manière de concevoir ou de structurer vos solutions de knowledge management (par exemple : droits d'accès, stockage, logs, données sensibles) ?
2. Avez-vous mis en place une politique spécifique de privacy by design dans vos cycles de développement produit ?
3. Quelles ont été les principales contraintes ou difficultés rencontrées pour atteindre (ou maintenir) la conformité RGPD en tant que start-up ?
4. Avez-vous ressenti un impact sur la relation client ou la stratégie commerciale à cause du RGPD (ex. : clauses contractuelles, réassurance, exportabilité) ?

II. Innovation produit et arbitrages technologiques

5. Est-ce que certaines fonctionnalités ont été modifiées, ralenties ou évitées pour des raisons de conformité ou de prudence vis-à-vis des régulations ?
6. À l'inverse, diriez-vous que la contrainte réglementaire a favorisé certains choix d'architecture ou de différenciation produit (par exemple en matière de sécurité, traçabilité ou transparence) ?
7. La conformité RGPD est-elle perçue en interne comme une valeur ajoutée ou plutôt comme un frein à la scalabilité ?

III. Positionnement stratégique et concurrence

8. Pensez-vous que les entreprises européennes comme Elium sont désavantagées par rapport à des concurrents non européens qui opèrent avec des obligations réglementaires plus souples ?

9. Le DMA s'adresse surtout à des grandes plateformes, mais pensez-vous qu'il pourrait avoir un impact indirect sur des acteurs B2B comme vous (interopérabilité, accès au marché, exposition aux grandes plateformes) ?
10. Avez-vous observé une différence dans les attentes réglementaires ou les perceptions client entre vos marchés belges, européens ou extra-européens ?

IV. Perspectives et rôle de la régulation

11. Pensez-vous que le cadre réglementaire européen actuel favorise ou freine l'émergence d'acteurs européens crédibles à l'international ?
12. Votre stratégie de développement a-t-elle été pensée pour répondre d'abord aux contraintes européennes, avant d'être exportée ailleurs ?
13. Quel type d'évolution réglementaire souhaiteriez-vous voir à l'avenir pour que la régulation accompagne l'innovation plutôt que la freiner ?

Conclusion

14. Quels conseils donneriez-vous à une start-up numérique européenne qui débute aujourd'hui et doit composer dès le départ avec le RGPD, le DMA et potentiellement le DSA ?
15. Avez-vous le sentiment que les régulateurs ou institutions européennes écoutent suffisamment les start-ups dans la définition des cadres législatifs ?

Appendix C.6. : Approach and interview questionnaire for a representative of Mistral AI (French start-up) for the third part of the thesis

Questionnaire – Représentant de Mistral AI – Intelligence artificielle, innovation et régulation européenne

Introduction pour l'entretien

Dans le cadre de mon mémoire de Master à l'UCLouvain, j'étudie l'impact combiné du Digital Markets Act (DMA) et du General Data Protection Regulation (GDPR) sur les

modèles économiques et les stratégies d'innovation des entreprises technologiques en Europe. Le positionnement de Mistral AI – entre excellence technologique, open source et souveraineté européenne – en fait un exemple central pour comprendre les opportunités et contraintes de l'innovation en IA face à la régulation.

I. Défis liés à la régulation des modèles d'IA en Europe

1. En tant qu'acteur européen de l'IA, quels sont pour vous les principaux défis posés par le cadre réglementaire européen (GDPR, DMA, AI Act) ?
2. Le GDPR affecte-t-il directement vos processus d'entraînement ou de déploiement de modèles ? Par exemple, sur les données utilisées pour entraîner vos LLMs ?
3. Comment Mistral intègre-t-elle les principes de privacy by design et de minimisation des données dans sa stratégie technologique ?

II. Innovation et contraintes techniques

4. Le respect du GDPR vous a-t-il conduit à écarter certaines sources de données, à modifier vos algorithmes ou à revoir votre infrastructure ?
5. Est-ce que cela crée un désavantage concurrentiel pour Mistral face à des acteurs non-européens (ex. : OpenAI, Google) ?
6. Pensez-vous que le cadre réglementaire européen pousse à développer une forme particulière d'innovation responsable ou éthique ?

III. Modèle open source et positionnement stratégique

7. Pourquoi avoir fait le choix de l'open source pour vos modèles ? Ce choix vous semble-t-il compatible avec les exigences du GDPR ?
8. Est-ce que le modèle open source est un avantage stratégique en Europe (transparence, souveraineté) ou une contrainte supplémentaire (contrôle, traçabilité des usages) ?
9. Voyez-vous une forme d'alignement possible entre régulation et innovation ouverte, ou craignez-vous un encadrement trop rigide de l'IA ?

IV. Europe comme terrain d'entraînement réglementaire ?

10. Est-ce que développer votre IA en Europe, dans un environnement réglementaire strict, constitue pour vous un avantage compétitif à long terme (ex. : conformité dès le départ, confiance des partenaires) ?

11. Votre stratégie produit ou vos partenariats ont-ils été influencés par la nécessité de rassurer les régulateurs ou les institutions publiques européennes ?

12. Envisagez-vous une adaptation différenciée de vos modèles selon les zones géographiques (ex. : Europe vs. États-Unis ou Asie) ?

Conclusion

13. Quels types de dialogue ou de coopération avec les régulateurs vous semblent nécessaires pour permettre à l'IA européenne de rester compétitive ?

14. Enfin, quel conseil donneriez-vous à une start-up IA européenne confrontée simultanément aux défis techniques, concurrentiels et réglementaires ?

Appendix C.7. : Approach and interview questionnaire for a representative of Odoo for the third part of the thesis

Questionnaire – Représentants d'Odoo – Régulation européenne, innovation et compétitivité

Introduction pour l'entretien

Je réalise un mémoire de Master à l'UCLouvain sur l'interaction entre deux régulations européennes majeures (le DMA et le GDPR) et leur impact sur les modèles économiques et la capacité d'innovation des entreprises numériques. Odoo, en tant qu'acteur européen majeur du logiciel open source, représente un cas particulièrement intéressant pour analyser les effets de ces régulations sur l'innovation, la conformité, et la compétitivité.

I. Conformité et gestion des données

1. En tant qu'éditeur de logiciels ERP, comment Odoo a-t-il intégré les exigences du GDPR dans ses produits et dans sa propre gouvernance interne ?
2. Le principe de privacy by design est-il appliqué dès la conception de vos modules ? Comment cela impacte-t-il vos cycles de développement ?
3. Quels sont les coûts humains et techniques liés à la mise en conformité au GDPR pour une entreprise comme la vôtre ?

II. Innovation et stratégie produit

4. Les contraintes réglementaires ont-elles un impact sur vos choix d'innovation (par exemple : fonctionnalités IA, modules RH, stockage cloud, interopérabilité) ?
5. Est-ce que certaines fonctionnalités ont été abandonnées, modifiées ou retardées pour conformité réglementaire ?
6. À l'inverse, ces régulations vous ont-elles permis de vous différencier stratégiquement vis-à-vis de concurrents non-européens ?

III. Concurrence, croissance et cadre européen

7. Le DMA vise des plateformes "gatekeepers" ; bien qu'Odoo ne soit pas concerné directement, est-ce que vous anticipez un impact indirect sur votre modèle économique ou sur vos partenaires intégrateurs ?
8. Pensez-vous que les régulations européennes comme le GDPR ou le DMA désavantagent les entreprises comme Odoo face à des acteurs américains ou chinois ?
9. Odoo ayant une forte croissance internationale, constatez-vous des différences d'obligations réglementaires entre régions (UE vs. US vs. autres) ? Comment gérez-vous cela ?

IV. Vision stratégique et prospective

10. Le fait d'avoir commencé en Europe vous a-t-il permis de développer une culture de conformité dès le départ, qui devient ensuite un avantage dans d'autres marchés ?
11. Pensez-vous que le cadre européen en matière de régulation numérique favorise ou freine la capacité des entreprises à innover ?
12. Quels leviers ou ajustements souhaiteriez-vous de la part des régulateurs européens pour stimuler l'innovation tout en protégeant les utilisateurs ?

Conclusion

13. En rétrospective, les régulations européennes ont-elles globalement freiné, accéléré ou réorienté votre stratégie d'innovation ?
14. Enfin, quels conseils donneriez-vous à une jeune entreprise numérique européenne confrontée aux régulations GDPR/DMA ?

Appendix C.8. : Approach and interview questionnaire for a representative of BEUC (European Consumer Organisation) and/or Test-Achats

Questionnaire – Représentant de Test-Achats / BEUC – Régulation numérique et protection des consommateurs

Introduction pour l'entretien :

Je réalise un mémoire de fin d'études à l'UCLouvain sur les effets croisés du Digital Markets Act (DMA) et du General Data Protection Regulation (GDPR) sur les marchés numériques européens. Au-delà des stratégies d'entreprise, je m'intéresse également à l'impact de ces régulations sur la transparence, les droits des utilisateurs, et la confiance dans les technologies. Votre point de vue, en tant que représentant des intérêts des consommateurs, est essentiel à cet équilibre.

I. Évaluation du cadre réglementaire du point de vue des consommateurs

1. Selon vous, le GDPR a-t-il permis des avancées concrètes pour les consommateurs en matière de protection de leurs données personnelles ?
2. Le DMA, bien qu'axé sur la concurrence, contient des dispositions utiles pour les utilisateurs (ex. : portabilité, désinstallation, interopérabilité). Ces mesures sont-elles suffisantes pour rééquilibrer la relation utilisateur–plateforme ?
3. Quels sont aujourd'hui les principaux manquements ou frustrations signalés par les consommateurs concernant le fonctionnement des grandes plateformes numériques ?

II. Régulation, pouvoir de marché et information du consommateur

4. Pensez-vous que les régulations européennes réduisent les asymétries d'information entre les plateformes et les consommateurs ?
5. Quels risques identifiez-vous si l'Europe n'avait pas adopté un cadre strict comme le GDPR ou le DMA ?
6. À l'inverse, voyez-vous un risque que la complexité réglementaire détourne les utilisateurs de leurs droits (ex. : demandes d'accès, consentements opaques, fausses fenêtres de choix) ?

III. Confiance, innovation et souveraineté numérique

7. Est-ce que ces régulations ont, selon vous, renforcé la confiance des utilisateurs envers les outils numériques en Europe ?
8. Le cadre actuel favorise-t-il une innovation au service des citoyens, ou reste-t-on encore dans une logique centrée sur les intérêts des grandes entreprises ?
9. Que pensez-vous de l'idée (issue de mon promoteur) selon laquelle certaines entreprises choisissent de se conformer d'abord aux standards européens pour ensuite aller à l'international ? Est-ce également bénéfique pour les consommateurs ?

IV. Vision future et recommandations

10. Selon vous, quelles améliorations prioritaires devraient être apportées au cadre actuel pour mieux protéger les consommateurs à l'ère de l'IA et des services personnalisés ?
11. La multiplication des textes (GDPR, DMA, DSA, AI Act…) rend-elle la compréhension difficile pour les citoyens ? Faut-il simplifier ou éduquer davantage ?
12. Quelles initiatives (transparence des algorithmes, labels, sanctions) pourraient vraiment changer la donne dans les prochaines années ?

Conclusion

1. Quels outils les associations de consommateurs ont-elles pour faire pression ou dialoguer avec les grandes plateformes numériques ?
2. Enfin, quelle grande leçon devrait retenir un jeune chercheur ou décideur qui s'intéresse à l'avenir des droits numériques en Europe ?

Appendix D.: Transtriction of interviews conducted

Appendix D.1. : Interview transcript with a the EU offical

[EU Official]
Ça ne peut pas être nommé dans la mémoire, et je crois que ça ne peut même pas être l'EDPB qui est nommé. Donc c'est évidemment pas une position officielle de l'EDPB, et l'EDPB en soi ne peut pas être nommé. En fait, on n'est pas censé même voir par le mémoire que l'IDPB a été interviewé.

Par contre, comme il faut quand même que vous puissiez utiliser ce qu'on vous dit, ce qu'on avait trouvé la dernière fois, c'était de dire... Vous écrivez en anglais votre mémoire ? On peut dire par exemple des entretiens avec des EU officials, ça marche.

Mais pas spécifiquement avec l'EDPB.

[Quentin Roland]
Je vais mettre mon ordinateur, comme ça on vous entend mieux. Vous me direz si vous m'entendez ou pas.

[EU Official]
Dites-moi, j'arrête la vidéo et je me mets plus près aussi, c'est possible ?

[Quentin Roland]
Oui, oui, c'est peut-être mieux.

[EU Official]
Alors on fait comme ça.

[Quentin Roland]
Donc voilà, je vais vous rappeler le contexte de mon mémoire. Donc j'analyse les effets combinés du DMA et du GDPR sur les marchés numériques européens. Et ma recherche s'inscrit dans une perspective multidimensionnelle, technologique par rapport au droit, par rapport à la stratégie d'innovation.

Et vise notamment à comprendre comment les entreprises réagissent en l'absence ou en complément des régulations claires. Donc cet entretien, dans le cadre de la deuxième partie de mon mémoire, vise à explorer ces zones sans régulation explicite. Et à comprendre le rôle effectif et stratégique de l'EDPB dans un tel contexte.

Donc, pour commencer, j'ai d'abord émis un premier point qui est la gouvernance des données dans un monde numérique en mouvement. Ma première question est, comment décririez-vous les principaux défis pour l'application effective du GDPR dans un environnement technologique aussi dynamique que celui des plateformes numériques ?

[EU Official]
Alors, c'est une question qui est assez générale. Je ne sais pas à quel point vous êtes familier du RGPD. Le RGPD, c'est une législation qui est basée sur certains principes.

Et ces principes sont censés s'appliquer à toutes les technologies. C'est-à-dire qu'on dit souvent que le RGPD est technology neutral. Et donc que les principes sont applicables, peu importe, disons, les évolutions des technologies dans nos temps.

Ça, c'est une première chose. En même temps, on se rend bien compte que, peut-être que je vais déjà un petit peu prendre de l'avance sur certaines autres questions, mais on se rend bien compte que pour certaines technologies, par exemple pour ce qui est de l'IA, on a aussi besoin d'avoir des règles spécifiques. La question, elle est après de se poser comment est-ce que ces règles spécifiques interagissent avec le RGPD.

Et c'est là que le travail des autorités de protection des données devient de plus en plus important, dans le sens où les différentes législations qui viennent s'ajouter au RGPD ne viennent pas remplacer le RGPD, mais au contraire viennent le complémenter, mais ils viennent le complémenter pas de n'importe quelle manière, ils viennent le complémenter en faisant référence à des concepts qui viennent du RGPD. Si je prends par exemple le cas du DMA, on a l'article 5.2 du DMA sur la nécessité d'obtenir le consentement des utilisateurs pour certaines combinaisons et cross-use of data. Ce consentement, il est clairement dit dans le DMA qu'il doit être obtenu de la même manière qu'il doit être obtenu sous le RGPD.

Donc les conditions du consentement qui viennent du RGPD sont exportées ou sont stétantes au consentement qui est demandé sous le DMA. Et donc on passe d'un système où les autorités de protection des données devaient déjà être cohérentes entre elles, devaient déjà avoir une interprétation générale de la protection des données et du droit de la protection des données pour ce qui est de l'application pure du droit de la protection des données. Plus on multiplie le nombre de textes qui font référence aux concepts qui viennent de protection des données, plus l'interprétation qui est faite par les autorités de protection des données devient importante pour aussi d'autres secteurs du droit qui agissent du droit de la concurrence avec le DMA, qui s'agissent du droit de la protection des consommateurs avec le DSA, ou de ce qu'on pourrait presque appliquer une régulation sectorielle avec AI. Je ne sais pas si ça répond un petit peu à votre question.

[Quentin Roland]
Oui, ça va. Ma deuxième question c'est, selon vous, quelles sont aujourd'hui les limites concrètes du GDPR face à des pratiques émergentes comme l'entraînement d'IA générative, la biométrie passive ou l'interopérabilité forcée ?

[EU Official]
Les limites du RGPD, je pense que si on regarde le rapport de la commission sur l'enforcement, sur la mise en vigueur du RGPD, ce qui revient souvent comme chose qui peut être améliorée, c'est la durée des enquêtes. Et en particulier en ce qui concerne les cas transfrontalisés. Dès qu'un traitement d'activité nécessite la collaboration de plusieurs autorités, il y a un certain nombre de mécanismes qui peuvent être mis en place et utilisés pour arriver à une décision cohérente, disons, et par l'ensemble des membres du public.

C'est sur ce point là que la commission dit qu'il y a moyen de s'améliorer. Pour ce qui est vraiment du contenu des textes, encore une fois, les principes du RGPD s'appliquent aux nouvelles technologies et on n'est pas vraiment limité. En appliquant le RGPD, on n'a pas vraiment le sentiment que les principes du RGPD ne peuvent pas être appliqués aux nouvelles technologies.

Cela ne veut pas dire qu'on ne peut pas clarifier les relations par exemple entre le RGPD et les autres textes. Et notamment si vous regardez dans le web-programme de l'EDPB, il y a un certain nombre de guidelines pour l'ensemble de ces textes qui sont prévus. Je pense que les guidelines entre DMA et GDPR, les guidelines entre AI Act et GDPR, les guidelines entre DSA et GDPR.

Donc le droit du RGPD en soi n'est pas dépassé. Est-ce qu'on peut encore clarifier comment ce droit s'applique par rapport aux autres textes ? Oui, bien sûr.

[Quentin Roland]

Ok, ça va. Ma troisième question dans cette thématique est que le GDPR repose beaucoup sur les principes de responsabilisation et d'accountability. Ces principes sont-ils suffisants en l'absence de régulations complémentaires comme le DMA et l'AI Act ?

[EU Official]
Est-ce que les principes d'accountability sont suffisants pour amener à une conformité avec le RGPD ? Les entreprises doivent se conformer à la loi, qu'il y ait ou non, qu'on parle ou non du principe d'accountability. Donc que ce soit le RGPD ou qu'on rajoute un autre texte, parce que là on va bientôt avoir le texte sur la Procedure of Regulation, qui rajoute des éléments de procédure.

La accountability, au-delà de dire que c'est le contrôleur qui est responsable, c'est aussi une manière de dire aux entreprises que cette responsabilité, vous devez être en mesure de la démontrer aux autorités. Non seulement vous devez vous conformer au droit, mais en plus de vous conformer au droit, vous devez être en mesure de démontrer que vous vous conformez au droit. C'est un ensemble d'actions et d'éléments que chaque contrôleur peut prendre pour démontrer à l'autorité qu'il s'est mis en conformité.

Est-ce que ça suffit ? On aimerait toujours avoir plus de moyens de s'assurer que les entreprises et que les organisations sont en conformité avec le RGPD. Mais il se trouve que le législateur a utilisé cette solution pour amener les entreprises à démontrer la conformité au RGPD.

Je ne sais pas si vous avez dans l'idée une autre manière de faire, mais d'avoir un autre texte qui dirait qu'il faut se mettre en conformité avec le RGPD aurait le même effet. La comptabilité, ce n'est pas dire qu'on s'en remet à ce que font les entreprises pour la conformité au RGPD. Les entreprises doivent respecter le RGPD, c'est la loi, c'est la base.

En plus de ça, la comptabilité demande qu'elles soient en mesure de démontrer leur mise en conformité par des moyens divers auprès des autorités. Oui, à mon sens, ça suffit.

[Quentin Roland]

Ok, ça va. On va passer à la deuxième thématique qui est la capacité d'action du régulateur et la coopération frontalière. Ma première question là-dedans, c'est le EDPB dispose-t-il aujourd'hui des moyens humains et techniques suffisants pour répondre aux défis posés par les entreprises de dimension globale ?

[EU Official]
Je ne m'aventurerai pas sur les EDPB seuls en tant qu'elles, mais ce qui est sûr, c'est que les autorités de protection des données et l'EDPB n'ont pas assez de ressources pour implémenter le droit de la protection des données. Donc il y a une prioritisation à faire. Ce n'est pas quelque chose qui est défini au niveau européen, mais on voit bien que les autorités nationales, que ce soit en Irlande, que ce soit en France...

[Quentin Roland]
J'allais justement y venir après.

[EU Official]
Ils se concentrent quand même sur les grandes plateformes. Et on comprend bien pourquoi, parce que c'est là que la plupart des utilisateurs sont. Constamment et régulièrement depuis de nombreuses années, les EDPB et les autorités de protection des données ont attiré l'attention sur le fait qu'elles manquent de ressources et qu'elles vont continuer à manquer de ressources, dans la mesure où, comme je l'ai expliqué au début, leur rôle s'agrandit.

[Quentin Roland]
Oui, tout à fait.

[EU Official]
Et qu'il y a de plus en plus de règles à faire respecter, y compris avec le Procedural Regulation qui arrive, mais aussi, comme je le disais, le DSA, le DMA et le AI act.

[Quentin Roland]

Quels sont les freins institutionnels ou juridiques qui empêchent une application uniforme du GDPR au sein de l'Union Européenne ?

[EU Official]
Vous me dites si vous voulez que je fasse un peu plus court pour la réponse, je ne sais pas combien de questions vous avez.

[Quentin Roland]
J'en ai 14 en tout, ça vaut de voir par rapport au temps que vous avez aussi.

[EU Official]
Et comme on a commenté un petit peu en retard, on peut faire jusqu'à 1 minute et demie, 45, quelque chose comme ça.

[Quentin Roland]
Oui, ça va, on est à la cinquième.

[EU Official]
Pour ce qui est des freins, il y avait beaucoup de freins procéduraux qui ont été expliqués dans ce qu'on appelle la EDPB Wish List. C'est ce document qu'on avait envoyé à la Commission et qui a donné lieu à la proposition de loi qui vient d'être adoptée pour les aspects procéduraux du RGPD. Il y avait un certain nombre d'éléments de droit national qui différaient d'un pays à l'autre.

Même si le RGPD s'applique partout dans l'Union Européenne de la même manière, chaque état membre conserve son droit procédural. Et il y a une certaine fragmentation des règles en termes de procédure qui empêche un enforcement cohérent. Je n'ai pas l'habitude de parler en français.

[Quentin Roland]
Il n'y a pas de soucis, monsieur.

[EU Official]
Les freins qui sont en train d'être adoptés, comment ça a enlevé certains de ces freins du point de vue de la procédure.

[Quentin Roland]
C'est justement ma prochaine question. La fragmentation dans les décisions nationales, par exemple avec le DPC irlandais et le VNIL français. Vous savez ce que c'est, je suppose ?

[EU Official]
Le DPC irlandais, oui, c'est le Data Protection Commission.

[Quentin Roland]
Et la Commission Nationale de l'Information et de la Liberté en France.

[EU Official]
Le Commissaire National Informatique et Liberté.

[Quentin Roland]
Est-ce que ça remet en question l'efficacité du GDPR en tant que cadre européen unique ?

[EU Official]
Ehhh non, ce dont je parlais avant, la fragmentation des règles, c'est une chose. C'est-à-dire que le droit français n'est pas le même que le droit irlandais. Et quand on fait une plainte sous le RGPD, ou une plainte basée sur le RGPD, même si la provision du RGPD sur laquelle la plainte se base est la même, le contentieux et la procédure de plainte ne sera pas la même.

On gagnerait à ce que ça soit harmonisé, et c'est ce que le règlement vise à faire. Par exemple, de manière très pratique, avoir un formulaire de plainte pour toutes les autorités de protection des données, qui demanderait toujours la même information, peu importe le pays, dans l'Union Européenne, ça permettrait aux autorités de partir déjà tous sur une

même date. C'est quelque chose qu'on avait proposé et qui, je crois, se retrouve dans la dernière version du texte.

Pour ce qui est des décisions qui sont prises par les autorités nationales, évidemment qu'elles ont une obligation de coopération entre elles, et donc l'idée c'est d'éviter d'avoir des décisions qui ne disent pas la même chose. Est-ce qu'en pratique, on a des décisions qui disent vraiment des choses très différentes ? Il faut voir au cas par cas.

Mais l'idée est que le RGPD a de toute façon suffisamment de mécanismes, on comprend suffisamment les mécanismes pour qu'on puisse arriver à une décision cohérente à la fin. Et là, je veux parler de l'article 60, le mécanisme de coopération, ou éventuellement l'article 65 pour une décision contraignante de l'EDPB au cas où les autorités nationales ne se mettent pas d'accord.

[Quentin Roland]
Mon troisième thème est les scénarios sans régulation claire et le rôle de l'EDPB. Dans des cadres où la régulation est encore floue, comme l'IA générative ou les métaverses, comment l'EDPB peut-il intervenir de manière proactive ?

[EU Official]
Avec des guidelines, avec des opinions. Il y a plusieurs de ces éléments pour ce qui est de Generative AI. Il y a aussi une guideline qui est annoncée dans le work program de l'EDPB pour ce qui est d'une pratique spécifique, qui est le scraping, qui est beaucoup utilisé pour l'intelligence artificielle.

Il y a aussi des guidelines qui sont en préparation. Après, l'EDPB, il ne faut pas oublier non plus que l'EDPB en tant que tel n'est pas un super régulateur. C'est-à-dire qu'à la différence de la commission, par exemple la commission va renforcer directement le AI Act, l'EDPB ne fait pas la loi, d'une part, et surtout ne rend pas des décisions sur des cas seuls.

C'est-à-dire que si un cas spécifique arrive devant l'EDPB, ça veut dire que les autorités de protection des données au niveau national n'ont pas réussi à se mettre d'accord. Jusqu'à maintenant, c'est quand même les autorités de protection au niveau national qui doivent prendre la décision. Dans ce sens-là, le rôle de l'EDPB se limite à fournir tout le support qu'on peut fournir à nos membres, essayer d'harmoniser leurs actions, mais à la fin, c'est toujours les autorités qui prennent les décisions.

[Quentin Roland]
Voyez-vous un rôle pour des mécanismes d'autorégulation ou de co-régulation dans la gouvernance des données à l'échelle européenne ?

[EU Official]
Je suis un peu moins porté sur le sujet. Ce qui me vient comme ça, ce serait les mécanismes de certification qui sont dans l'RGPD.

[Quentin Roland]
Ma prochaine question touchait à ça, justement. Le recours à des standards techniques ou des certifications comme les codes de conduite ou GDPR CARPA pourrait-il devenir un levier plus important dans les prochaines années et sous quelles conditions ?

[EU Official]
Comme je n'ai pas d'informations publiques ni de position de l'EDPB là-dessus, j'aurais du mal à vous donner la réponse claire. Ce qui est sûr, cependant, c'est que les certifications et les codes de bonne conduite n'ont pas beaucoup été utilisés jusqu'à maintenant. Est-ce qu'ils peuvent avoir une place plus importante ?

Oui, parce qu'on ne se permet presque pas à servir. Est-ce que c'est dans les plans des autorités de protection des données d'utiliser cet outil ? Ça, je n'ai pas d'informations.

[Quentin Roland]

Ok, très bien. Mon quatrième point sont les perspectives et évolutions du cadre réglementaire. Le GDPR est parfois perçu comme un freinateur pour l'innovation, en particulier chez les startups.

Partagez-vous ce constat et comment concilier innovation et protection pour vous ?

[EU Official]
Personnellement, je ne pense pas que... Tout dépend de ce qu'on entend par frein à l'innovation. Si la régulation est un frein à l'innovation, alors le RGPD est un frein à l'innovation.

Si on considère que l'innovation n'est une innovation que si elle respecte un certain nombre de normes et de principes, c'est-à-dire qu'on veut innover, mais on ne veut pas innover n'importe comment, et on ne veut pas innover en mettant en danger les droits des personnes, alors le RGPD n'est pas un frein. Il y a même un argument à faire que, en étant à l'avant-garde des textes du jour, en étant la norme qui régule dans le plus de détails les activités de traitement de données, le RGPD impose un modèle qui, au-delà de l'Europe, est réutilisé sur d'autres continents. Il y a une sorte de soft power qui se diffuse, disons, et où les entreprises qui sont en Europe se mettent en conformité avec le RGPD et en faisant cela, elles se garantissent aussi de respecter les réglementations qui sont inspirées du RGPD et qui reprennent ces principes un peu partout dans le monde.

Si on a une vision à court terme, on peut dire que me mettre en conformité avec ces règles, ça me demande de l'argent, ça me prend du temps, c'est un frein pour l'innovation. Si on prend une perspective un peu plus globale et qu'on voit l'impact qu'a eu le RGPD dans le monde, on peut aussi le voir presque comme un avantage compétitif.

[Quentin Roland]
L'articulation entre le GDPR et d'autres régulations sectorielles comme le DMA, le DSA, l'AI Act, est-il aujourd'hui bien intégré dans les travaux du comité ? Quel risque de chevauchement ou de conflit y voyez-vous ?

[EU Official]
Le risque de chevauchement ou de conflit est limité en tenu du fait que la plupart des textes dont vous parlez font des références explicites au RGPD et définissent leur position par rapport au RGPD. Si on prend par exemple l'AI Act, il dit clairement que le texte s'applique sans préjudice du RGPD. Pareil pour ce qui est du DMA, pareil pour ce qui est du DSA.

Il y a évidemment des situations où il y aura des overlaps, et c'est pour ça que les guidelines sont là pour préciser comment appliquer les règles en pratique. À quel point c'est intégré dans les travaux du EDPB ? Ça l'est de plus en plus puisqu'on se rend compte que les autorités de protection des consommateurs et les autorités de la concurrence sont en demande de l'expertise des autorités de protection des données et se rendent compte que sur des sujets aussi vastes et transversaux que les sujets numériques, on a besoin de l'action pour les régulateurs de manière collective.

Ce n'est pas soit l'EDPB, soit l'autorité de protection des données, soit protection des consommateurs. C'est collectivement s'atteler à un problème et discuter pour rendre des décisions qui vont dans le même sens. Une chose qui est intéressante de regarder, c'est dans le DMA, il y a le DMA High Level Group, qui est un organisme, une réunion organisée par la commission, qui rassemble autour de la table les autorités de protection des consommateurs, les droits de la concurrence, les autorités de protection des données et les régulateurs télécom.

Quand tous ces gens sont autour de la table, on se réunit à vacances régulières et on se parle évidemment et on se donne des informations sur ce sur quoi on est en train de travailler pour s'assurer que si on travaille sur la même chose, on dit des choses qui sont, si pas similaires, à minimum, à minima, disons, cohérentes et qu'on ne se contradisent pas. Donc, de plus en plus, les autorités sont conscientes du besoin d'avoir une coopération entre différents types d'autorités.

[Quentin Roland]

A votre avis, quel ajustement serait nécessaire pour renforcer l'efficacité du GDPR dans les années à venir, en particulier dans le contexte technologique extrême ou non prévu initialement ? Si vous pensez qu'il y en a un.

[EU Official]
Je pense que pour pouvoir répondre à la question de ce qu'on pourrait améliorer dans le RGPD, il faudrait déjà être en mesure d'avoir une ressource d'appliquer les règles. Je pense que du point de vue des autorités, l'enjeu principal, c'est de donner les moyens aux régulateurs de faire leur travail. Une fois que les régulateurs auront ces ressources, on sera en mesure de dire ce qui peut être amélioré.

Sachant que ça ne nous a pas empêché de déjà le faire avec cette wish list de l'EDPB, et que ça ne nous empêche pas de voir que cette nouvelle procedure regulation va aussi dans le bon sens, et de continuer de dire à la commission, si vous voulez faire tel texte ou tel texte, on pense que ça peut être utile. Évidemment, le travail ne s'arrête pas, parce qu'on n'a pas toutes les ressources, mais si je devais choisir qu'un seul enjeu pour dire que ça, c'est ce qui empêche la protection des données, d'être encore mieux respecté et appliqué, ce serait définitivement la projection des ressources.

[Quentin Roland]
Il me reste deux petites questions pour conclure. En un mot, selon vous, quels sont les risques majeurs si l'Europe ne parvient pas à compléter ou adapter son arsenal réglementaire face aux évolutions numériques ?

[EU Official]
Le risque majeur si on ne complète pas notre arsenal numérique ? Encore une fois, je ne suis pas persuadé que ce soit en ajoutant des textes, qu'on arrivera à une meilleure mise en conformité. Le risque, c'est simplement que les droits des personnes soient encore moins respectés.

La mission de l'EDPB, c'est de supporter les autorités de protection des données pour que les droits des personnes soient respectés. Elles le font dans une certaine mesure avec les

ressources qui sont les leurs, et comme on l'a dit, en se concentrant sur les grandes plateformes, mais pas seulement. Par exemple, si je pense à l'acné, je sais qu'il y a beaucoup de cas qui sont relatifs à une ou deux personnes.

Donc, il ne faut pas non plus penser que les autorités de protection des données ne regardent que les grands cas. Oui, le risque, c'est toujours le même. Le risque, c'est de voir les droits des personnes à la protection des données pas foués, disons.

[Quentin Roland]
Ma dernière question, quel rôle voyez-vous pour l'EDPB dans le futur des marchés numériques, arbitrage juridique, coordination technique ou organes stratégiques plus globales ?

[EU Official]
Alors ça, j'aimerais bien le savoir pour être tout à fait. Le premier c'était quoi, pardon ?

[Quentin Roland]
Arbitrage juridique, coordinateur technique ou organes stratégiques ?

[EU Official]
Coordinateur technique et arbitrage juridique, l'EDPB le sera toujours, puisque c'est dans le RGPD. L'EDPB est là pour résoudre les disputes entre les autorités de protection des données et en même temps fournir tout le support nécessaire pour qu'il y ait une coopération technique entre ces autorités. Stratégique aussi, parce qu'avec le programme de travail ou avec le timing qui est celui de l'EDPB, donc le fait que les guidelines souvent prennent du temps mais sont étalés sur peut-être un ou deux ans, et en fait que le travail est planifié plusieurs années à l'avance, il y a des priorités, il y a des piliers qui sont identifiés dans le programme de travail de l'EDPB, et donc il y a aussi une dimension stratégique, je ne crois pas qu'on ait à choisir vraiment entre un de ces trois. Les trois viennent du RGPD en fait.

[Quentin Roland]

Ok, très bien, voilà, c'était tout pour mes questions, merci beaucoup, c'était très intéressant. Aurevoir

Appendix D.2: Interview transcript with a legal expert and professor of European law at UCL – Alain Strowel

[Alain Strowel]
voilà bonjour, dites moi en quoi je peux vous être utile.

[Quentin Roland]
donc merci d'avoir répondu présent à cette interview, je vais un peu vous expliquer le contexte, donc voilà je fais mon mémoire et je suis en master 2 à la LSM et je réalise un mémoire sur l'impact combiné du DMA et du GDPR sur le marché numérique européen et mon objectif c'est d'examiner dans quelle mesure ces deux régulations influencent les modèles économiques et les stratégies d'innovation des entreprises qui opèrent dans l'union européenne. donc j'avais besoin de votre expertise dans le cadre de ma deuxième partie de mon mémoire qui analyse les risques liés à l'absence de régulation ainsi que les scénarios alternatifs notamment l'autorégulation et du coup je souhaitais bénéficier de votre expertise en droit européen et en plus particulièrement sur les mécanismes juridiques d'autorégulation

[Alain Strowel]
d'autorégulation, c'est très vaste votre approche, donc je ne sais pas dans quelle mesure je pourrais être utile, mais on peut essayer de préciser vos questions, surtout que l'autorégulation c'est plus tellement juridique, c'est à la limite en dehors du droit, donc en plus mais bon

[Quentin Roland]
d'abord est-ce que vous me permettez de vous enregistrer?

[Alain Strowel]

oui mais alors vous l'utilisez uniquement pour votre recherche parce qu'en plus c'est un sujet que je ne possède vraiment pas très bien, DMA GDPR c'est une combinaison assez particulière, donc honnêtement vous pouvez enregistrer mais je pense qu'il n'y aura pas énormément que vous pourrez en retirer, j'ai accepté l'interview mais je ne suis pas un expert du DMA, je ne suis pas non plus un expert du GDPR, alors la combinaison des deux c'est vraiment très étroit, mais bon je vous écoute,

[Quentin Roland]
ok donc mon premier thème était le cadre général et la vision juridique, selon vous quels sont les risques principaux liés à l'absence de régulation publique dans les marchés numériques notamment en matière de concurrence et de protection des données?

[Alain Strowel]
oui mais donc les deux règlements que vous envisagez là ont des objectifs très différents, puisque le GDPR le RGPD vise essentiellement un créer un marché unique en ce qui concerne les données, à faciliter la circulation des données et à conférer des droits aux individus, donc ça n'a rien à voir avec une régulation comme le DMA qui envisage en fait de faire de la régulation de la concurrence ex-ante, donc c'est un tout autre objectif, conférer des droits, protéger la vie privée et assurer un marché d'un côté et de côté réguler le marché par une autorité ex-ante, c'est difficile à rendre compatible, ce sont des blocs très différents, donc il n'y a pas de convergence a priori dans les objectifs et en plus ce sont malheureusement comme toujours des législations qui sont, je n'ai pas vérifié ça dans le DMA, donc on a dit dans le DMA que c'est certainement sans préjudice de l'application du RGPD, donc il y a des points de contention, oui de contentieux possible entre les deux, mais ça s'est laissé ouvert à ceux qui doivent implémenter et ce sont des autorités très différentes d'ailleurs, les autorités en matière de vie privée d'un côté et en tout cas pour les gatekeepers, une autorité comme la commission qui s'occupe de la concurrence, mais c'est vrai qu'il y a une convergence entre certaines problématiques en matière de vie privée et la problématique de la régulation du marché, ça c'est sûr, c'est un peu le sujet sur lequel vous vous appuyez, si on discute, je ne suis pas un expert du P ou OK modèle par exemple, oui ça c'est un peu la régulation d'un modèle qui lui-même a des implications sur le marché et des implications pour la vie privée, le modèle du Pay or Okay

imposé par META par exemple, donc c'est vrai que dans votre mémoire vous vous concentrez par exemple sur le modèle du Pay or Okay, peut-être intéressant parce que c'est un exemple qui est à l'intersection des deux, donc je pense que ce sera intéressant d'utiliser des use case tels que celui-là, sur lequel il y a par ailleurs eu aussi des décisions en matière de concurrence, donc pas DMA mais concurrence ex poste, notamment en Allemagne, donc voilà ça permet de bien illustrer votre problématique en tant que juriste, on aime bien repartir d'un use case, ça pourrait être celui-là, mais je ne sais pas si vous l'envisagez

[Quentin Roland]
pourquoi pas, ok très bien, ma deuxième question est le modèle européen repose en partie sur une régulation ex ante comme vous l'avez dit et des droits fondamentaux dans le GDPR, quels seraient selon vous les impacts d'un modèle purement autorégulé ?

[Alain Strowel]
Oui donc un modèle autorégulé ça veut dire d'abord autorégulé par qui ? parce que on peut concevoir l'autorégulation de manière étroite ou de manière large, si c'est une autorégulation uniquement par l'industrie et encore ça pourrait être même une partie de l'industrie, ça pourrait être par exemple les plateformes, les petites et les grandes, mais l'industrie il y a beaucoup d'autres partenaires, parce que justement ces plateformes travaillent avec énormément d'autres business et il y a des relations B2B, donc autorégulation simplement sur le secteur business plateforme ou bien autorégulation en général dans les relations B2B et puis alors vous avez évidemment d'autres partenaires qui sont impliqués comme les consommateurs en B2C et on les inclut aussi dans le processus d'autorégulation, enfin voilà donc je pense qu'il faudrait préciser alors quel niveau d'autorégulation vous envisagez, parce que effectivement ça risque d'être de l'autorégulation entre soi qui ne tient pas compte d'autres intérêts commerciaux de tous ceux qui doivent travailler avec ces plateformes qui sont devenus indispensables pour faire du commerce en ligne par exemple.

[Quentin Roland]

Comment les principes du droit européen encadrent-ils ou limitent-ils les mécanismes d'autorégulation dans le secteur du marché numérique ? Je ne sais pas si vous savez répondre à cette question ou pas.

[Alain Strowel]
Je ne suis pas sûr de tout posséder là, il y a généralement dans le cadre européen une invitation à une forme d'autorégulation, mais c'est de l'ordre de l'invitation parce qu'effectivement on préfère à priori ce modèle là, mais il n'y a pas de mécanisme qui en général pousse à ce qu'il y ait une autorégulation. Ça fonctionne pour certains secteurs, bon il y a des exceptions, par exemple sur tout ce qui concerne la désinformation, la commission pendant longtemps a poussé à l'adoption d'un code de pratique qui a été adopté par les grandes plateformes sur la désinformation et après ça a été rendu quasi obligatoire parce qu'il y avait la menace de prendre un règlement sur le sujet. Dans certains cas particulièrement délicats où il y a un intérêt public en jeu, alors vous avez un lien qui est établi entre une autorégulation accompagnée et une autorégulation qui devient quasi obligatoire avec un bâton qu'utilise la commission disant on va rendre obligatoire et alors si ça devient obligatoire vous êtes soumis aussi aux sanctions par exemple dans le DSA parce que ça ça concerne plutôt le contenu donc c'est le Digital Service Act mon exemple là. Donc ça c'est un exemple que je connais un tout petit peu ce rapport entre autorégulation et régulation en ce qui concerne les information disorders comme on les appelle ou la désinformation mais je pense qu'il n'y a pas d'équivalent sur les règles de fonctionnement du marché. Vous avez identifié des codes d'autorégulation des plateformes d'ailleurs ?

[Quentin Roland]
Pour l'instant non mais c'est d'un point de vue totalement extérieur et d'après les recherches que j'ai pu avoir sur internet mais je ne peux pas en conclure qu'il n'y en a pas.

[Alain Strowel]
Il y a notamment le self-preferencing, ce qu'on appelle le self-preferencing c'est peut-être aussi un point vous pourriez essayer de voir ce qu'il y a dans des... oui je pense pas que

vous allez trouver ce code d'autorégulation mais il y aura peut-être des mission statements de certaines sociétés qui diront on va pas faire du self-preferencing.

[Quentin Roland]
Mon deuxième thème est l'autorégulation comme une solution juridique viable ? L'autorégulation est-elle selon vous une alternative crédible au niveau européen pour encadrer les pratiques des grandes plateformes numériques et si oui à quelles conditions ?

[Alain Strowel]
Non moi ça ne me paraît pas une alternative crédible pour la raison principale c'est qu'on a de grands opérateurs qui ne sont pas localisés en Europe et donc on n'a aucun levier si ce n'est le droit à leur égard. Je pense qu'un système d'autorégulation peut fonctionner s'il rentre dans un cadre par exemple national classique avec des opérateurs nationaux qui sont établis dans un cadre national et où vous avez un environnement et à ce moment là on peut laisser mais il y a tout un cadre autour parce que au niveau européen les autorités européennes n'ont pas beaucoup de pouvoir finalement par rapport au pouvoir d'un état normal dans sa juridiction et ici on a en plus des opérateurs qui sont basés à l'étranger donc je pense que c'est en fait dans un cadre tel que celui là avec des pouvoirs moindres pour l'autorité publique donc l'autorité européenne d'un côté et des opérateurs qui sont établis en dehors ça suffit certainement pas.

[Quentin Roland]
Quelle différence faites-vous entre autorégulation co-régulation et soft law dans le contexte du droit européen ?

[Alain Strowel]
Oui moi je pense que ce sont des termes qui sont assez mal définis et il n'y a pas de définition en tout cas en droit il n'y a pas de définition vous avez des documents de la commission qui peuvent être des communications au better regulation et qui vont essayer de distinguer les trois niveaux mais les trois niveaux sont alors autorégulation, co-régulation et régulation. Soft law pour moi c'est un peu un synonyme d'autorégulation

mais enfin c'est pas tout à fait correct non plus je suis d'accord en fait il faudrait alors avoir peut-être dans votre typologie donc régulation, co-régulation, autorégulation et puis au même niveau que l'autorégulation vous auriez alors soft law bon ce sont des recommandations, il y a différents instruments qui peuvent alors être considérés comme soft law sans être de l'autorégulation. La notion de soft law peut couvrir de l'autorégulation peut couvrir d'autres instruments parce que l'autorégulation suppose que ce sont quand même des guidelines qui ont été établis par les partis et soft law ça peut être établi aussi par des autorités publiques ou par des tiers pas des autorités publiques vous imaginez peut-être encore des tiers mais du point de vue juridique ça a la même valeur que de l'autorégulation je ne sais pas si c'est suffisamment clair mais je ferais plutôt ça comme distinction.

[Quentin Roland]
Existe-t-il des exemples dans ou hors du numérique où l'autorégulation s'est révélée efficace en Europe?

[Alain Strowel]
Oui alors il y a certains pays qui connaissent davantage cette approche là c'est je pense typique du Royaume-Uni mais bon on n'est plus dans l'Union Européenne donc oui donc je pense que ça marche relativement bien dans un pays comme le Royaume-Uni en tout cas dans un cadre où vous avez des acteurs nationaux je pense notamment dans le domaine des médias, la régulation des médias qui devient d'ailleurs aussi des médias électroniques donc qui font partie un peu des marchés dans ce cadre là aussi longtemps que les acteurs sont des acteurs justement qui sont basés dans le pays qui pratique l'autorégulation à l'égard des acteurs encore établis dans le pays ça fonctionne je pense c'est une tradition qui fonctionne mieux dans les pays anglo-saxons mais bon c'est fort inconnu par exemple en France parce qu'en France c'est un pays plus centralisateur on a une tradition justement qui va un peu à l'inverse de l'autorégulation il y a des nuances selon les pays mais je pense que les pays anglo-saxons les pays nordiques aussi ça marche mieux il y a beaucoup de conditions qui sont requises pour que l'autorégulation fonctionne bien donc c'est complexe il faut une certaine culture aussi dans ce qui n'est pas acquis nécessairement partout je pense que ça marche nettement mieux aussi dans les

pays anglo-saxons au royaume uni qu'aux états unis enfin on doit pas non plus négliger ce rôle aux états unis.

[Quentin Roland]
Donc vous pensez pas que ça fonctionnerait chez nous par exemple ?

[Alain Strowel]
mais en plus c'est compliqué à faire fonctionner dans une une entité comme l'europe où vous avez encore des états nationaux avec des règles différentes donc l'autorégulation dans ce cadre là alors que certains pays vont peut-être prendre des mesures qui sont contradictoires avec des règles d'autorégulation qui sont pas partagées dans les autres pays ça n'a pas ça peut pas bien fonctionner dans un cadre européen où on a déjà même pas là une convergence suffisante au niveau des cadres hard law de la régulation c'est devient encore beaucoup plus compliqué d'avoir un système d'autorégulation qui fonctionne

[Quentin Roland]
ok mon troisième thème est l'application à la technologie aux plateformes du coup quels sont les enjeux juridiques associés à des pratiques comme l'interopérabilité technique la publicité comportementale ou le profilage algorithmique dans un cadre sans régulation ?

[Alain Strowel]
oui je pense que là il ya des risques importants je n'ai pas retenu votre liste là de problèmes mais il y en a au moins deux deux deux parmi ceux que vous citez qui invoquent les droits et qui impliquent les droits fondamentaux et donc je pense que mais tout dépend encore à quel niveau l'autorégulation est faite mais comme on avait dit au départ on peut avoir des notions plus ou moins large d'autorégulation bon si c'est l'autorégulation simplement par les plateformes ce sera quand même difficile de tenir compte suffisamment des droits fondamentaux des utilisateurs donc si on fait de l'autorégulation qui implique les organismes de consommateurs par exemple on peut l'imaginer dans certains cas je pense que ça peut être fait en incluant les organismes de consommation mais c'est à mon avis pas concevable dans votre cadre là aussi du numérique global ?

[Quentin Roland]
ok que dit le droit européen actuel sur la responsabilité des plateformes lorsque aucune régulation sectorielle n'existe ?

[Alain Strowel]
oui alors la règle générale c'est la règle qui a été adoptée déjà où les règles ce sont celles des exonérations de responsabilité donc ça ça a été l'approche aux états unis dans le dencency act là de 1996 et puis on a grosso modo introduit la même règle dans la directive sur le commerce électronique les articles 12 à 15 qui maintenant se retrouve aux articles 4 8 du DSA parce qu'ici on n'est plus tout à fait dans le domaine dma vous glissez je pense un peu sur la question de la responsabilité pour du contenu et là c'est plus dsa donc mais l'approche qui est celle des années 90 lorsqu'on avait une industrie de l'internet tout à fait naissante ça a été de protéger cette industrie en prévoyant des exonérations mais conditionnées de responsabilité mais des exonérations quand même lorsqu'on a revu les règles qu'on a transporté dans le DSA on n'a pas changé ce cadre alors qu'évidemment le rôle des intermédiaires a fondamentalement changé depuis là le milieu des années 90 à aujourd'hui et que maintenant on voit que il ya différentes catégories d'intermédiaires à l'époque on visait les intermédiaires techniques c'était les opérateurs de télécom etc parce qu'il y avait de la jurisprudence qui considérait qu'ils pouvaient être responsables et aux états unis ça peut coûter très cher et donc on a introduit cette règle d'exonération d'abord aux états unis et puis on a peut-être un peu suivi de manière je dirais un peu trop servile et sans se rendre compte qu'on a un tout autre cadre en europe où les d'abord les risques pour les intermédiaires opérateurs télécom etc n'étaient pas les mêmes puisqu'on n'a pas du tout la même approche sur les sanctions les damages les dommages et intérêts qu'aux états unis alors on a on a introduit ces exonérations là dans la directive de 2000 qui font déjà moins que dans le cadre européen et on les a encore maintenu alors que on a le web 2.0 ou 3.0 selon la façon de compter avec des opérateurs qui n'ont plus de rôle essentiellement technique quand une plateforme fait de l'hébergement comme facebook c'est pas simplement l'opération technique qui était envisagée dans les années 90 où votre opérateur télécom pouvait aussi héberger 10 mégas et vous offrait 10 mégas d'espace pour remettre votre contenu quand on a ces grandes plateformes qui font de

l'hébergement comme youtube ou toutes les plateformes de méta c'est quand même autre chose donc oui on a un cadre qui n'a pas suffisamment tenu compte de l'évolution des intermédiaires notamment des hébergeurs

[Quentin Roland]
ok pensez vous que des plateformes comme tiktok ou méta pourraient s'autoréguler efficacement sans intervention publique pourquoi ou pourquoi pas ?

[Alain Strowel]
Mais bon ils font un effort parce que par exemple méta vous le savez a introduit le oversight board qu'on a considéré comme étant la cour suprême de l'internet ou à tout le moins la cour suprême du groupe méta et les autres ont un peu suivi parce qu'il fallait effectivement apparaître aussi clean et avoir son système interne qui est une forme d'autorégulation bon c'est pas tout à fait critiquable parce que je pense qu'il y a une assez grande indépendance de l'oversight board par exemple au sein du groupe méta qui peut prendre des décisions qui ne sont pas nécessairement les décisions qui plaisent au manager du groupe et à Mark Zuckerberg donc effectivement il y a une certaine indépendance mais finalement bon le nombre d'affaires etc c'est vraiment la cerise sur le gâteau ce qui est important c'est qu'on est un peu plus de transparence sur les pratiques qui sont celles de tous ceux qui prennent la décision sur la modération du contenu mais de nouveau ici on rentre de nouveau dans une question qui est un peu différente c'est plutôt de nouveau DSA que DMA parce qu'on parle de contrôle du contenu etc

[Quentin Roland]
je vais parler du DSA mais j'essaie quand même de le limiter dans mon mémoire DMA ou GDPR parce que sinon il y a aussi l'AI Act dont je pourrais parler, prochaine question, le droit européen pourrait-il évoluer vers une reconnaissance formelle du mécanisme d'autorégulation dans le domaine des données ou de la concurrence numérique?

[Alain Strowel]
oui mais de nouveau là je vois pas exactement ce qu'on pourrait envisager alors qu'on a un cadre de régulation parce que le RGPD est quand même très contraignant justement là

on a un cadre qui va peut-être à certains égards un peu loin donc il faudrait d'abord simplifier et alléger le RGPD pour qu'il y ait alors des pratiques peut-être qui puissent être adoptées comme des modèles de conduite par des codes d'autorégulation mais on a un système assez dense de régulation un système d'exigence de compliance qui va assez loin qui ne tient pas suffisamment compte d'ailleurs de la taille différente des entreprises et donc ça il faut d'ailleurs parler de ça c'est que si vous comparez DMA et RGPD d'un côté on a une régulation qui tient compte de la taille de l'entreprise c'est une approche graduée et qui est centrée sur les grands opérateurs les gatekeepers où il y a des problématiques de marché qui sont importantes de ce côté là et qui ne s'appliquent pas à des petits opérateurs de même le DSA c'est aussi une approche graduée ce qui est je pense positif le RGPD ignore tout à fait la question de la taille et du pouvoir de marché puisqu'il impose les mêmes obligations pour un petit opérateur c'est une startup avec deux ou trois types et une grande entreprise il n'y a pas de gradation dans les obligations mais bon ça peut se justifier parce que les droits fondamentaux doivent être respectés évidemment par tout le monde mais voilà ça c'est ça c'est le problème de l'interférence des questions droits fondamentales qui ne permettent pas toujours une approche graduée je pense qu'on évolue parce que vous avez peut-être suivi que justement il y a des intentions de la commission d'alléger le RGPD et d'introduire une approche graduée c'est une avec des règles particulières pour les SME en allégeant les règles pour le SME ça c'est intéressant parce que ça tient compte alors d'une position sur le marché et qui était une considération tout à fait non pertinent dans l'approche du RGPD jusqu'à présent on ne tient pas compte de la position sur le marché de la puissance et de la dominance de l'entreprise on pourrait davantage en tenir compte si les règles du RGPD sont appliquées et donc là ça deviendrait peut-être plus convergent avec une approche qui tient compte de la taille de la puissance de marché des entreprises comme le DMA ou le DSA.

[Quentin Roland]
Dans un contexte post DMA RGPD pensez vous qu'un retour partiel à des logiques de co-régulation pourrait être envisagé ?

[Alain Strowel]

Oui co-régulation oui ça je crois que ça peut fonctionner justement dans la mesure où il y a en dernière instance la possibilité d'une régulation et même de sanctions qui sont relativement importantes alors dans ce cadre là même des opérateurs étrangers qui parce que je pense que l'autorégulation ça fonctionne quand on est un peu entre soi dans un cadre qui est déterminé et donc à ce moment là compte tenu de la possibilité de passer éventuellement de la régulation classique avec des sanctions éventuellement substantielles ça peut être un incitant suffisant même pour des opérateurs rétablis à l'étranger pour s'engager dans un processus de co-régulation oui oui.

[Quentin Roland]
D'où vient ma prochaine question, quel garde-four serait juridiquement nécessaire pour rendre ce type de mécanismes compatibles avec les droits fondamentaux ?

[Alain Strowel]
Oui mais alors oui moi je l'envisageais plutôt du côté de la régulation du marché donc et là c'est moins clair donc côté DMA et là c'est moins clair qu'il y ait des droits fondamentaux impliqués est-ce que ça peut fonctionner pour des domaines où les droits fondamentaux sont vraiment en jeu ça me paraît plus compliqué donc oui la co-régulation peut fonctionner dans le champ du dma je serais plus sceptique pour ce qui concerne le rgpd et je vois d'ailleurs pas vraiment comment on pourrait mais j'ai déjà dit tout à l'heure passer du niveau régulation à un niveau de co-régulation dans le secteur vraiment de la vie privée ça je crois que c'est tout à fait utopique et inconcevable ce qu'on peut essayer d'éviter c'est certaines frictions entre les l'approche des tech companies et toute cette éthique des ingénieurs je pense et des commerciaux aussi qui dirigent cette industrie dans laquelle en fait tout frein à l'utilisation des données est mal vu donc pour un ingénieur toutes données doivent pouvoir être partagées éventuellement utilisées pour entraîner un modèle il ya cette éthique dans le domaine je des ingénieurs des technophiles et qui est tout à fait contradictoire avec l'approche des droits fondamentaux que ce soit un droit de propriété intellectuelle qui est aussi un droit fondamental où le droit fondamental à la vie privée où on essaie de limiter la possibilité d'accéder de partager pour des raisons qui sont justifiables donc ça je pense que c'est irréconciliable et il y a un énorme travail en général du côté des ingénieurs et des computer scientists etc mais il n'y a pas l'éthique qui

est c'est pas une éthique compatible avec celle des droits fondamentaux donc c'est irréconciliable pour moi

[Quentin Roland]
J'ai deux petites questions pour finir et conclure du coup selon vous dans quelle mesure l'autorégulation peut-elle ou non constituer une réponse suffisante aux enjeux actuels des marchés numériques européens ?

[Alain Strowel]
oui mais donc je pense que voilà j'y ai déjà répondu je vais répéter là voilà non

[Quentin Roland]
Ma dernière question alors si vous aviez un conseil à formuler aux institutions européennes en matière de gouvernance future du numérique qu'elle serait-il ?

[Alain Strowel]
Ah oui ce serait d'abord de peut-être de légiférer moins d'attendre un peu plus et peut-être oui on a maintenant beaucoup d'obligations ex-ante il faudrait voir si la multiplication de ces obligations ex-ante n'est pas disproportionnée dans certains cas donc d'attendre peut-être davantage et justement peut-être de trouver des mécanismes pour inviter les parties à faire d'abord ainsi c'était un champ dans lequel on n'a pas de régulation donc pour des problèmes admettons futur qui n'est pas été envisagé de d'essayer d'y aller progressivement en passant peut-être par un stade d'autorégulation puis de co-régulation plutôt que d'aller comme on a fait très très vite en matière de AI vers la régulation enfin bon voilà il y avait des codes de conduite mais je pense que on aurait pu encore attendre un peu plus et on découvre maintenant toutes les difficultés de mise en oeuvre par exemple de AI act mais bon okay c'est un autre sujet.

[Quentin Roland]
ok ça va merci beaucoup pour votre temps et vos réponses très intéressante

[Alain Strowel]

Bonne continuation bonne chance dans votre mémoire éventuellement vous me l'envoyez là si vous vous en rappelez quand ce sera terminé merci voilà

Appendix C.4: Interview transcript with a professor in innovation UCL-Anonymous

[Professor in innovation]
Rappelez-moi le contexte, parce que je passe d'un rayon à l'autre.

[Quentin Roland]
Donc mon mémoire touche à tout ce qui est l'interaction entre le Digital Market Act et le GDPR et leur impact sur les modèles économiques et les capacités d'innovation des entreprises dans le marché européen. Et du coup, votre expertise sur les stratégies d'innovation pourrait être précieuse pour que je comprenne comment les entreprises peuvent s'adapter dans ce contexte réglementaire. Donc voilà, on va commencer avec mes premières questions.

Le premier point que je voulais aborder, c'est est-ce que les régulations et innovations, est-ce que c'est une tension ou une opportunité ? Selon vous, dans quelle mesure les réglementations européennes DMA et GDPR freinent-elles ou stimulent l'innovation dans les entreprises européennes ?

[Professor in innovation]
Je n'ai pas une connaissance pointue de ces deux réglementations. Je peux vous parler de réglementations en général, pas de ces réglementations-là en particulier. Sauf que c'est peut-être déjà un des enjeux, c'est que ce sont deux réglementations qui sont assez complexes.

Et donc un premier enjeu, c'est ça. Cette complexité, elle peut à la fois créer de la peur en disant on ne sait plus rien faire, c'est trop compliqué, etc. Mais elle génère en tout cas un coût.

Donc il y a des coûts de compliance, de se dire finalement ça me prend du temps de comprendre ce qu'il en retourne, d'éventuellement vérifier si chez moi dans mon fonctionnement je suis compliant, et puis d'assurer le fait que je reste compliant, que mes collègues ne commencent pas à faire des choses qui sont interdites, etc. Je connais un gars sur internet, il peut trouver des adresses e-mails, etc. Ou bien se dire zut, cet outil qu'on utilise depuis des années, en fait si on creuse, on n'est pas tout à fait compliant ou il y a un risque.

Donc il y a un premier élément qui est une notion de coût, de compréhension, d'analyse et de mise en conformité quelque part. Donc ça c'est un premier élément. Maintenant le miroir de ce coût, c'est que ça peut être vu comme une barrière à l'entrée, c'est à dire que pour être actif dans mon domaine, il faut maîtriser ça.

Et qu'est-ce qu'on enseigne en management? Est-ce que c'est bon d'avoir une barrière à l'entrée dans une industrie? Oui.

Si vous êtes dans une industrie où n'importe quel amateur peut entrer et faire son truc, si vous avez une barrière d'entrée très basse, en fait c'est mourrait pour vous. Et donc voilà, vous voulez faire une API sur OpenAI ou sur ChatsGPT et faire un agent qui fera ça, il y a juste deux mille autres personnes qui sont en train de faire la même chose. Et donc là il y a déjà un premier paradoxe, entre guillemets, ou un premier compromis.

Oui, ça génère des coûts, mais le fait qu'il y ait des barrières à l'entrée, qu'il y ait des coûts, est aussi quelque part une barrière à l'entrée et fait en sorte que ceux qui maîtrisent ces réglementations ont un avantage quelque part par rapport à ceux qui ne les maîtrisent pas. Le cas extrême, c'est la réglementation bancaire qu'on a mis en place suite aux crises financières qui crée des coûts de compliance tels que seules les grandes banques arrivent à gérer ça. Et donc on a vu une concentration et des tas de petites banques avoir des difficultés et des startups fintech qui rentrent là-dedans, il n'y en a plus beaucoup parce qu'il y a un coût fixe de compliance qui est élevé.

Donc ça c'est un premier élément. Il y a un deuxième élément qui est la question de l'enforcement, c'est-à-dire il y a une réglementation d'accord, mais est-ce qu'elle est appliquée? Est-ce que si mon concurrent ne l'applique pas, il y a de fortes chances qu'il soit dénoncé ou détecté?

C'est un peu le restaurateur qui est obligé de faire du noir parce que tout le monde fait du noir. Et donc même si moi je ne veux pas en faire, mes concurrents en font. Pour la petite histoire, il y a très longtemps, pour les restaurants universitaires de Louvain, on avait évalué le coût réel d'un repas et c'était du genre 20 euros parce que tout était fully compliant, tout le monde était déclaré, etc.

Et donc ça coûtait moins cher d'aller en face, de prendre un plat dans un restaurant en face et de le donner aux étudiants que de le faire, mais parce qu'il y a des coûts de compliance. Donc c'est une vieille histoire. Donc ça c'est une deuxième question, c'est l'enforcement.

Ce que je vous ai dit avant sur la barrière à l'entrée, ce n'est valable que s'il y a effectivement un enforcement et que si mon concurrent ne respecte pas la règle, il se fait coincer. Ça c'est un premier élément. Il y a un deuxième élément qui est la question de clarté, c'est-à-dire quand on innove, on fait des nouvelles choses par définition, et la question c'est est-ce qu'on peut le faire, ou est-ce que dans deux ans on va me dire qu'on ne peut pas, ou bien un jour quelqu'un va m'attaquer et je vais perdre le procès.

Et donc là de nouveau il y a un effet positif et négatif. Il y a un effet négatif qui est que les réglementations vont définir un certain nombre de choses qu'on peut faire ou qu'on ne peut pas faire. Il y a parfois des réglementations positives, des réglementations négatives.

Il y a des réglementations où tout ce qui n'est pas expressément interdit est autorisé, et il y en a d'autres où non, voilà juste ce que vous pouvez faire et rien d'autre. Donc ça c'est un premier élément. Je ne pourrais pas vous dire le DMA et le RGPD dans quelles catégories ils sont, mais c'est un point important.

Et donc lorsqu'on essaie de réglementer par rapport à l'innovation, on essaie d'anticiper les usages possibles et dangereux, et de définir un cadre par rapport à ça. Et fatalement on va parfois se tromper. Il y a des usages, quand on a défini les droits de propriété intellectuelle, même sur le web, personne n'a pensé au cas quid d'une IA qui va pas copier-coller le contenu, mais qui va tout bouffer et en faire autre chose.

Voilà l'exemple où la réglementation sur les droits d'auteur, elle a été remise à jour à l'ère digitale, et quand on a fait ça, on n'a pas anticipé qu'il y aurait cette option. Et donc maintenant c'est une énorme discussion. Est-ce que le fait d'aller poacher vos contenus pour nourrir un modèle de machine learning, est-ce que c'est du fair use ou pas?

Si on y avait su à l'époque, on l'aurait défini comme oui c'est du fair use, ou non c'est pas du fair use. Donc fatalement une réglementation va se tromper, va devoir faire des hypothèses sur le futur qui seront parfois réelles, parfois pas vraies, et donc ça peut dans certains cas poser des contraintes. De se dire, on nous a interdit de faire ça, alors que dans d'autres pays on peut le faire, ou dans d'autres pays en théorie on ne peut pas le faire, mais c'est pas a force, et donc on est dans une logique de concurrence éloignée.

Donc il y a deux aspects, il y a un, la réglementation m'empêche de faire quelque chose qui serait très utile, c'est juste qu'ils n'y aient pas pensé, donc c'est interdit pour le moment, et la réglementation m'empêche de faire quelque chose que mes concurrents internationaux peuvent faire. Et donc ça c'est deux effets négatifs, pour vous donner un exemple de nouveau, pas dans ce cas-là, mais donc D'Erbigom, il y a quelques années a mis au point, donc D'Erbigom, vous voyez, ils font les isolations de toit, ils ont inventé un roofing bio, donc un roofing entièrement sans bitume, et puis quand ils ont voulu le faire autoriser aux Pays-Bas, la catégorie de produits s'appelle bitumine based products, donc produits au bitume, et donc ils ne savaient pas mettre le leur, puisque ce n'est pas à bitumine base, et donc la catégorie dans laquelle ils vous aident n'existait pas, si vous n'existez pas, l'assurance ne vous couvre pas, si l'assurance ne vous couvre pas, aucun client va vous acheter.

Donc il y a cette idée de, voilà, l'effet négatif c'est de nouveau blocage imprévu, non désiré, et concurrence éloignée. L'effet positif, c'est l'effet de clarté, de se dire, ok, voilà le terrain de jeu, je sais maintenant, je peux faire des investissements, je peux faire, et donc là, un exemple de nouveau, qui n'est pas des meilleurs GPD, c'est tout ce qui est marché des quotas CO2, qu'est-ce qui sera dedans, qu'est-ce qui ne sera pas dedans, si plusieurs entreprises ensemble économisent une tonne de CO2, qui pourra dire que c'est moins, ce sera à quel prix, tout ça est probablement en train d'être, et tant que ça n'est pas clair, les entreprises ont du mal à investir, l'incertitude, elle augmente le coût du capital, et si vous avez plus de coûts du capital, vous avez moins à investir, et donc il y a toute une série d'endroits où les entreprises sont demandeuses d'une réglementation, d'un cadre, ou fait qu'on aboutisse, parce que, dites-nous dans quel jeu on va jouer, et pour vous donner un autre exemple, Johnson et Johnson à Baird, près d'Anvers, a fait de la géothermie, donc ils ont creusé un trou de un kilomètre et demi pour aller chercher de la température et de la chaleur pour chauffer leur installation, et bien le projet a perdu plusieurs années, parce qu'il n'y avait pas de réglementation sur, est-ce qu'on peut creuser à un kilomètre et demi de profondeur, et exploiter ce terrain, en fait il y avait une législation jusqu'à quelques centaines de mètres, qui vous disait, ça c'est à vous, vous pouvez faire ce que vous voulez, mais plus bas il n'y avait pas, et ils ont été à la commune qui leur a dit, je sais pas, ils ont été à la province qui leur a dit, je sais pas, etc.

Et donc là, l'absence de réglementation a fait qu'ils ont perdu du temps, si on leur avait dit, non vous pouvez pas, on arrête, et oui vous pouvez, j'y vais, mais par contre je vais pas creuser pendant un kilomètre et demi pour qu'après mon voisin m'attaque en justice, et qu'on me dise, en fait vous pouviez pas, donc vous voyez les deux effets positifs et négatifs, en fait en donnant un cadre, on peut se tromper et donc on aura des opportunités, ou bien on donne un cadre qui s'applique qu'à vous, et alors vous avez la concurrence déloyale, mais dans l'autre sens, donner un cadre, voilà maintenant je sais ce que je peux faire, et dans le domaine du, il y a un troisième élément, c'est que le cadre peut aussi être une source d'avantages concurrentiels, ça veut dire que si je suis, si je peux garantir à mes clients, si vous travaillez avec moi, je suis RGPD compliance, et donc vous le serez aussi, ça c'est un avantage concurrentiel, il y a peut-être que moi qui sais le faire, mais bien sûr pour ça, ça suppose qu'il y ait une réglementation, tandis que si vous disiez, chez moi, vos

données sont safe, et que le concurrent disait, chez moi aussi, oui mais moi c'est vraiment safe, tandis que lui pas, ben non, le RGPD, et d'autres choses, dit, ça c'est safe, ça c'est pas safe, c'est comme si vous dites, si je suis ISO compliance, tout le monde sait ce que c'est, c'est validé par des tiers, etc, donc le fait qu'il y ait un cadre, peut aussi donner une source d'avantages concurrenciers, s'il n'y a pas de cadre, l'entreprise qui voudrait se différencier sur base de, par exemple, la privacy, Apple a été longtemps un peu perçu, se positionne toujours comme un acteur chez qui la privacy est sûre, mais si Samsung dit au client, moi aussi, vous donnez son safe chez moi, il faut être expert, ou il faut, pour comprendre, si oui, mais est-ce que c'est vraiment vrai, ou oui, pas vraiment, et donc la réglementation fournit un signal, un signal qui permet de dire, moi je suis vraiment, par exemple, privacy, tandis que l'autre pas, et le client peut aussi se dire, ah oui, lui il est RGPD compliance, enfin RGPD c'est pas comme c'est obligatoire, c'est un peu, mais par exemple, ces logiciels sont RGPD compliant, donc si je mets mes données privées dans ces logiciels, je resterai RGPD compliant, tandis que l'autre ne l'est pas, ah mais je sais faire la différence, donc ça peut être, c'est une source d'avantages concurrentiels, c'est une source de différenciation, et donc ça permet au marché entre guillemets de mieux fonctionner, puisque quelqu'un a l'opportunité de se différencier là-dessus, tandis que s'il n'y a pas de règle, c'est comme les gens qui vous disent carbone neutral, ou carbone ceci, ou bio, tout le monde dit qu'il est bon pour la santé, il y en a où c'est vrai, d'autres où c'est pas vrai, mais ceux qui le sont vraiment, ils ne savent pas se différencier, parce que l'autre le dit aussi, c'est un vieux papier en économie qui parle de market for lemon, c'est les voitures d'occasion, vous pouvez aller revoir ce papier, en fait une voiture d'occasion, le client ne sait pas dire si elle est bonne ou pas bonne, il n'y a pas de règle qui dit ça c'est une voiture que vous pouvez vendre, ça vous ne pouvez pas vendre, qu'est-ce qui se passe quand c'est comme ça, les honnêtes qui vendent vraiment des bonnes voitures, qui sont fatalement plus chères, disparaissent du marché, puisque le client ne sait pas voir la différence, chez vous c'est une voiture qui coûte 10 000, chez vous c'est 5000, oui mais chez moi elle est vraiment safe, l'autre aussi, il me dit qu'elle est safe, je vais à celui qui le fait à 5000, et donc ce sont les escrocs qui restent, et donc fatalement, imaginez, il n'y aurait pas l'RGPD, il y aurait plein de gens qui vous diraient, venez chez moi, vous donnez son C, vous n'en faites pas, le moins cher, c'est celui qui ferait moins attention, c'est un peu comme le restaurant qui vous sert de la bouffe périmée, qui ne fait pas attention au chaud, il aura des coûts plus

bas, et donc ils pourront vous vendre le kebab un peu moins cher, donc la réglementation peut aussi être une source d'avantages concurrentiels et de différenciation, donc ça c'est un élément supplémentaire, le dernier élément qui est peut-être le plus important, c'est que l'objectif de la réglementation, c'est aussi de balancer les intérêts des différentes parties prenantes, de se dire dans un marché non régulé, le plus fort et plus malin gagne, celui qui sait écraser les autres et celui qui sait faire croire aux autres qu'il est le meilleur, va gagner, et donc celui qui est fait, ou celui qui n'est pas assez malin ou informé pour comprendre qu'il se fait plumer, il va se faire avoir, et donc le but de la réglementation, c'est aussi d'éviter ça, donc d'éviter qu'il y ait des abus de position dominante, d'éviter que des clients ou des usagers se fassent avoir, et aussi éviter, parce qu'il n'y a pas que protéger les clients, il y a protéger la société en général, il y a éviter que moi en fait je veux bien donner mes données à un tel gars et je m'en fiche si elles ne sont pas privées, mais attention, grâce à ça, il met en place des outils etc, où en fait vous donnez accès à votre pc, sauf que dans votre pc il y a les photos de tous vos amis et eux n'ont pas donné leur accès, mais tant pis c'est trop tard, donc le dernier et peut-être le plus important rôle de la réglementation, c'est en fait de trouver un équilibre entre la liberté d'entreprendre et la propriété privée, qui sont les deux principes fondamentaux, on peut argumenter que ce sont les deux principes fondamentaux du capitalisme, mais ça d'un côté, et de l'autre côté vous avez finalement les droits fondamentaux des personnes, et en fait s'il n'y a pas de règles, il n'y a aucune garantie que le marché et son libre fonctionnement vont protéger les droits fondamentaux, on peut trouver plein d'exemples faciles, le cas où ce n'est pas possible, ou parce que le marché n'est pas équipé, le marché est équipé pour être paraitre optimale par rapport à l'utilité perçue, si vous vous rappelez votre cours de microéconomie, il est efficace, mais son efficacité est dans un sens extrêmement étroit, on ne parle que que d'utilité perçue mesurée, et il ne faut pas oublier quand on dit efficace, ça veut juste dire paraitre optimale, ça veut dire qu'il n'y a pas moyen de faire gagner une personne sans en faire perdre une autre, et donc une situation où j'ai tout et vous n'avez rien, est paraitre optimale, parce que la seule manière que vous n'avez plus, c'est de me prendre à moi, donc vous voyez qu'on a eu le cerveau un peu lavé par cette idée d'efficacité, et donc on nous bascine que le résultat sera meilleur si on laisse le marché fonctionner, ce n'est pas vrai du tout, le fonctionnement marché a énormément de bénéfices, notamment en termes d'expérimentation, d'exploration etc, mais il n'y a

aucune garantie que le résultat de tout ce bouillonnement soit optimal pour la société dans son ensemble, et donc regardez ce qui se passe en intelligence artificielle, ou bien au niveau des crypto monnaies, on voit deux environnements assez dérégulés, on peut réglementer, ça donne l'effet positif énormément d'expérimentation, d'entrepreneuriat etc, mais par contre ça donne des effets réellement ou potentiellement extrêmement dommageables, d'abord pour toute une série de clients, le nombre de gens qui se sont fait plumer sur des plateformes de crypto monnaies, mais aussi sur la société en général, les externalités, les risques d'instabilité financière, la manipulation des médias, etc, donc c'est le dernier point de mon argumentation, mais c'est peut-être le plus important, mais le problème c'est qu'on l'a un peu oublié. Dans le discours public, réglementation c'est vu comme péjoratif, c'est de l'administration, mais ça c'est un discours politique, la civilisation n'existe que s'il y a des institutions, et les institutions ne peuvent exister que s'il y a des règles. Dans mon cours, je montre aux étudiants le désert de l'Atacama au Chili, qui est l'endroit le plus sec au monde, et je leur dis, là il n'y a aucune réglementation, donc ça devrait être un paradis d'innovation, ou bien vous pouvez aller dans la bande de Gaza ou en Iran, là il n'y a plus rien qui fonctionne, il n'y a plus de gouvernement, il n'y a plus de réglementation, parce que c'est vraiment le paradis de l'innovation, de l'entrepreneuriat, et donc il faut se rappeler que des bonnes réglementations pour créer un marché, pour faire fonctionner un marché, pour défendre les différents acteurs de son marché, c'est indispensable. En fait il n'y a pas d'innovation, il n'y a pas d'entrepreneuriat sans réglementation. Et donc la question maintenant c'est, c'est quoi une bonne règle ?

Et une bonne règle, ce n'est pas facile à définir, pourquoi ? Parce que cette question d'incertitude dont on a parlé, de prévoir un peu tous les cas d'usage et toutes les évolutions, et puis aussi parce que bonne, c'est un avis subjectif. Bonne, ça dépend pour qui ?

Le droit de grève, est-ce que c'est bon ou pas bon ? Ça dépend pour qui ? Le droit à la vie privée, est-ce que c'est bon ou pas bon ?

Donc vous avez maintenant par exemple, pour ce qui est de la protection des données, des entreprises qui ont réussi à mettre en danger tout ce qui est de Whistleblowing, en

positionnant ça comme de l'atteinte à la confidentialité des données. Et donc ils ont mis en place une loi, soi-disant, qui est présentée comme protégeant les entreprises de vols d'informations et de données, ce qui en soit est une bonne chose, sauf qu'une des conséquences de cette loi, c'est que quelqu'un qui serait un Whistleblower, pourrait enfin être condamné comme divulgant des informations confidentielles de l'entreprise et donc des secrets d'affaires. Vous voyez, c'est une loi qui avait sans doute des bonnes raisons d'exister, mais qui a aussi des effets secondaires.

Est-ce qu'ils étaient prévus ? Est-ce que c'est de la manipulation ? Est-ce que c'est des effets secondaires imprévus ?

Je n'en sais rien, mais c'est quoi une bonne réglementation ? Ça dépend du point de vue. Et donc, quand quelqu'un vous dit, est-ce qu'il faut interdire le 5G à Bruxelles ?

Ou est-ce qu'il faut protéger les taximènes du Uber ? C'est quoi une bonne décision dans ces questions-là ? Ça dépend de qui vous êtes.

Donc, c'est aussi une des raisons pour lesquelles définir des bonnes réglementations, c'est difficile, parce qu'en fait, il n'y a pas de consensus sur qui est bon. Et donc, on essaie de tenir compte de l'intérêt général. Et l'intérêt général, il est défini par qui ?

Il est défini par des pourparoles, des gens qui se défendent comme étant porteurs de l'intérêt général, nommés par qui, légitimés par qui, etc. Quand vous avez la réglementation chimique, vous avez le lobby de l'industrie chimique et vous avez Greenpeace, aucun des deux n'a été élu. Et tous les deux, on peut challenger leur légitimité, de dire qui êtes-vous pour parler au nom de...

On a vu ça en France lors de la discussion sur la réglementation, justement, des aspects bio et tout. Des gens se sont présentés comme défenseurs des petits agriculteurs. Et donc, du coup, ils étaient très populaires.

En fait, c'était des grosses exploitations. C'était des gens qui n'avaient jamais mis les pieds dans un champ, qui avaient des milliers d'hectares. Mais en se présentant comme le défenseur des petits agriculteurs, alors tout d'un coup, tout le monde était d'accord avec eux.

C'est comme quand on parle de taxation des plus-values ou de l'immobilier en Belgique. On dit toujours « Ah, mais la pauvre petite pensionnée qui a son petit immeuble et qui vit son loyer, vous allez la mettre en danger ». Ah oui, oui, peut-être ça, oui.

Donc il y a une question de... Les réglementations doivent tenir compte de toutes les parties prenantes. Et ça, c'est très difficile à mettre en œuvre, puisque ces parties prenantes, elles sont multiples, elles sont contradictoires et elles n'ont pas nécessairement de porte-parole validé.

C'est tout le fonctionnement de la démocratie, c'est ça. Il y a un dernier point qui est à fois un trade-off. C'est la notion de souveraineté.

Alors, c'est ce que je veux dire par ça. En fait, une règle, elle est définie par une autorité publique qui agit sur un territoire. Mais l'innovation et l'entrepreneuriat, lui, il n'est pas nécessairement attaché à un territoire.

Et donc, une des grosses raisons pour lesquelles il n'y a pas plus de grosses start-up digitales en Europe, c'est parce que le marché européen est beaucoup plus fragmenté que le marché américain et le marché chinois. Vous avez Amazon, FedEx et le dollar, vous avez 300 millions de clients. Vous avez la même chose, vous avez Bolt.com aux Pays-Bas, il doit fonctionner en 15 langues différentes. Ce qu'il peut vendre en France, ce n'est pas la même chose que ce qu'il peut vendre en Allemagne, etc. Donc, il y a cette question de fragmentation. Et donc là, le fait d'avoir des réglementations, en tout cas au niveau européen, ça peut avoir un effet positif parce que ça défragmente.

Si cette réglementation européenne, elle remplace des réglementations nationales ou régionales en Belgique, ça, c'est un effet positif. Parce que pire qu'une réglementation,

c'est deux réglementations. En Belgique, comme on est des champions pour découper notre confetti en petits morceaux encore plus petits, il y a des tas de domaines où il y a une réglementation wallonne, une réglementation bruxelloise, une réglementation flamande.

Et ça, du point de vue de l'entrepreneuriat ou de l'innovation, avoir trois réglementations au lieu d'une, c'est d'office pas bon. Et donc ici, si c'est plus de réglementations au sens plus de réglementations locales, régionales, nationales, ça fragmente encore plus le marché. Donc, je pense que c'est toujours le cas.

Il y a quelques années, les vaccins qu'un bébé doit avoir de 0 à 2 ans ne sont pas les mêmes en Belgique qu'en France, en Italie. On dirait qu'un bébé, c'est un bébé. Et la réglementation sur qu'est-ce qui est un bon vaccin, qu'est-ce qui est un mauvais vaccin, pour moi, en Europe, on devrait s'être mis d'accord.

Ah ben non. Mais donc, pour des vendeurs de vaccins, il ne faut pas les manquer. Donc, si même pour les vaccins, on n'arrive pas à se mettre d'accord, pensez aux services digitales, etc.

Et donc là, l'obstacle, la réglementation a un effet négatif si elle est définie localement, régionalement, nationalement, parce qu'elle multiplie la fragmentation. Et donc, pour l'innovation, l'entrepreneuriat, c'est des barrières. Par contre, si la réglementation peut être créée au niveau européen, alors ce serait encore mieux mondial, mais dans le contexte actuel, c'est compliqué.

Là, alors, tout d'un coup, on a le marché unique, qui est aussi un sujet qu'on a oublié. Le marché européen a été créé pour la paix et pour la croissance économique. Et la croissance économique, elle venait du fait que c'est un marché unique.

Si j'ai le droit de fonctionner en Belgique, je peux vendre en Grèce, en Finlande. En fait, ça, on l'a un peu oublié. Et donc, ces deux règlements-là, s'ils peuvent remplacer des

réglementations nationales et régionales par une réglementation qui est la même au niveau européen, ça, c'est très bien pour l'innovation et l'entrepreneuriat.

Parce que, je répète, c'est une des barrières principales. Donc là, c'est une vraie histoire. Il y avait un Amazon en Belgique qui s'appelait Proxys, qui a commencé en Belgique francophone, et qui avait le site web, le paiement, la logistique, tout ça.

Et puis, on doit aller en Flandre. En Flandre, ce n'est pas les mêmes bouquins en flamand. C'est d'autres bouquins et d'autres CD.

Donc, il fallait... On va aller en France. En France, le prix du livre est réglementé.

Vous ne pouvez pas vendre un livre moins cher. Je veux aller en Allemagne. C'est encore autre chose.

Donc, toutes ces startups, en particulier digitales, se heurtent tout de suite à des barrières. Dans le domaine des... On revient pour la banque.

C'est un des obstacles. C'est qu'une entreprise, avant, devait avoir des licences bancaires dans chaque pays, avec des règles différentes. Et que ça, c'est un coût de compliance énorme.

Voilà. Donc ça, c'est peut-être le dernier argument. C'est ce côté fragmentation qui a aussi un effet.

Et peut-être qu'on peut trouver... Il y a un contre-argument. C'est toujours un trade-off.

C'était un papier qui a été publié il y a une vingtaine d'années. Donc la fragmentation européenne des réglementations crée un obstacle à l'entreprise à l'innovation. Mais elle est aussi une barrière à l'entrée.

Et donc l'argument à l'époque, c'était que si on simplifie les règles européennes, ceux qui allaient en bénéficier, c'étaient les entreprises américaines. Parce qu'elles avaient des rendements d'échelle. Et ça avait fonctionné très très bien.

Mais pour elles, pour le moment, le marché européen était beaucoup trop compliqué. Et donc seules les entreprises européennes arrivaient à fonctionner. Donc on revient sur l'argument de départ.

C'est une barrière à l'entrée. La multiplicité des règles en Europe est une barrière à l'entrée. Ceux qui les maîtrisent sont capables d'opérer en Europe.

Alors ceux qui ne la maîtrisent pas... Certaines entreprises alimentaires ou chimiques américaines ne peuvent pas opérer en Europe parce qu'elles ne maîtrisent pas la réglementation. Ça, quelque part, ça protège.

Et de nouveau, cette protection, elle est peut-être légitime ou elle est peut-être aussi du protectionnisme. Et ça, ça nous amène... Ça, c'est un point supplémentaire.

C'est que ces règles nationales ou régionales ou européennes, ceux qui sont favorables disent que c'est pour protéger l'environnement, les citoyens, la Suisse, etc. Et d'autres vont dire que ces règles peuvent aussi être utilisées comme du protectionnisme. Et donc c'est pour rendre la vie difficile aux entreprises non européennes pour entrer sur le marché.

Et donc c'était l'exemple de l'Allemagne qui avait des règles très très strictes sur les ingrédients qu'on pouvait mettre dans de la bière. Et donc résultat, les grands brasseurs européens, Belges en particulier, ne pouvaient pas entrer sur le marché allemand. Alors soi-disant, c'était pour protéger la santé des Allemands, mais de facto...

Et en général, de nouveau, c'est un peu gris. De facto, si vous dites pas de GMO en Europe, ça empêche les entreprises championnes du GMO, des OGM, d'entrer et donc ça protège

les entreprises européennes. Donc ça a un effet protectionniste, mais ça a aussi un effet de dire qu'on ne veut pas d'OGM parce qu'on trouve que c'est dangereux pour la santé, etc.

Donc il y a aussi un danger ou un enjeu. Ces réglementations, RGPD, DMA, peuvent être vues comme une protectionnisme et certains l'ont vu comme une manière de mettre des bâtons dans les roues dans les gros players américains et chinois et pour donner une chance aux players européens d'émerger. Donc ça peut aussi être vu comme de la politique industrielle, je pense.

[Quentin Roland]
Ok, ça va. Vous avez un peu répondu à mes deux prochaines questions, mais je vais quand même les évoquer. Du coup, le concept de Compliance Driven Innovation est parfois évoqué.

Est-il crédible dans la pratique ou reste-t-il une exception ?

[Professor in innovation]
On verra ce qu'on a dit. Si on crée des nouvelles règles, des nouveaux défis, ceux qui innovent pour mieux y répondre, ça peut stimuler l'innovation. Tandis que si la règle n'existait pas, il n'y a personne qui se fatiguerait à faire ça.

Si demain on vous dit qu'il faut faire des frigos qui possèdent des produits chimiques qui détruisent l'ozone, et le jour où on a dit que c'était interdit, les gens ont dû inventer des frigos sans fluorocarbone. Je ne sais plus si c'est fluorocarbone, mais ce n'est pas important. Du coup, les gens ont dit qu'ils avaient une technologie sans fluorocarbone.

Avant, tout le monde s'en fichait. Maintenant, on dit que la technologie n'intéresse pas.

[Quentin Roland]
Le principe de Privacy by Design est imposé par le GDPR. Est-il perçu par les entreprises comme une opportunité d'innovation ou comme une contrainte technique ?

[Professor in innovation]
Il faut leur demander, mais on revient à mon avis, sans doute les deux. Les entreprises n'aiment pas qu'on leur dise ce qu'elles doivent faire, mais en même temps, ça a tous les avantages dont on a parlé avant.

[Quentin Roland]
Maintenant, on va passer à mon deuxième point qui est les modèles économiques et les stratégies d'adaptation. Observez-vous des transformations de modèles économiques directement liées à l'entrée en vigueur des deux directives ?

[Professor in innovation]
Je n'ai pas l'exemple comme ça, mais on peut quand même imaginer que par exemple, tout ce qui est lié à la publicité, à la collecte de données, ces règles sont susceptibles de rendre certains modèles impossibles ou de demander à d'autres. Pour vous donner un exemple, c'est notamment Google qui a poussé sur le fait qu'on enlève les cookies. En fait, c'est parce qu'ils savent détecter qui vous êtes sans cookie.

Rien qu'en combinant votre usage, la manière dont vous tapez sur votre clavier, etc. Et donc, quelque part, ils n'ont plus besoin de cookie. Mais en faisant ça, ils tuent tous ceux qui en ont besoin.

Donc, c'est clair que changer les règles, ça va être favorable à certains joueurs, défavorable à d'autres, et ça va permettre de mettre en place des nouvelles tactiques de jeu. C'est comme si vous enlevez le hors-jeu au foot. Tout d'un coup, les tactiques de jeu vont changer.

Donc ici, oui. Je n'ai pas l'exemple. Enfin, si, il y a l'exemple Google que je viens de vous dire, mais qui n'est pas directement lié à GPD.

Mais il est clair que quand vous changez les règles, vous rendez certains modèles obsolètes, vous rendez d'autres plus intéressants et vous donnez l'opportunité à de nouveaux modèles d'exister.

[Quentin Roland]
Ok. Est-ce que certains secteurs ou types d'acteurs, exemple open source, plateforme, software, service, start-up, AI, s'adaptent mieux que d'autres?

[Professor in innovation]
Oui, sûrement. Je pense qu'il y a peut-être un flou. On revient sur la complaince et la compréhension.

C'est qu'on fait croire aux gens que le RGPD veut dire qu'on ne sait plus rien faire. Non. C'est comme le principe de récaution.

On dit que ça veut dire qu'on doit vivre dans une grotte. Non. Par exemple, dans le B2B, il y a beaucoup de confusion avec les données qui ne sont pas des données de personnes privées.

Vous pouvez faire des tas de choses. On parle du legacy. Celles qui ont des vieux systèmes qui n'avaient pas prévu ça, elles ont du mal à s'adapter.

Celles qui ont des systèmes où je peux dire que j'envoie un email à tout le monde, je demande qu'ils acknowledge, qu'ils m'autorisent. C'est bon. Oui, c'est clair qu'il y a des entreprises qui peuvent plus facilement s'adapter que d'autres.

[Quentin Roland]
Le DMA peut-il, selon vous, inciter certains acteurs à ajuster leur stratégie de croissance ou leur architecture de service pour éviter la désignation comme gatekeeper? Parce que c'est ça tout l'enjeu du Digital Market Act, qui est pour désigner une plateforme numérique qui détient une position dominante.

[Professor in innovation]
Ça, ça touche à un autre effet négatif. Quand on parlait des effets imprévus des réglementations, on disait qu'on n'avait pas prévu cet usage. L'autre effet imprévu, ce sont

des comportements opportunistes, où à partir de 50 employés, j'ai une représentation syndicale, je vais rester à 49.

On revient un peu dans les effets de bord, dans les effets non désirés. Beaucoup de réglementations ont un périmètre défini, par exemple défini par la taille. Elle crée comme effet pervers que la barrière à l'entrée dont on parlait tantôt, elle augmente soudainement dès qu'on passe ce seuil, et ça peut induire comme effet pervers que les entreprises ne vont pas vouloir passer ce seuil, voire vont créer des constructions pour ne pas le passer.

C'est un peu, on rajoute une règle, mais il y a des gens qui trouvent une astuce pour contourner la règle. Tout ça c'est inefficace, parce que ça rend le système moins efficace, mais dans l'intérêt des individus, pour échapper à la règle, je fais comme ça. Il y a des effets, je n'ai pas d'exemple particulier sur le DMA, mais sur le principe des réglementations en général, il y a des effets de bord non désirés.

[Quentin Roland]
Mon troisième point, c'est l'Europe versus le reste du monde. Est-ce qu'il y a des avantages compétitifs ? Ma première question là-dedans, est-ce que vous avez identifié des cas où les entreprises européennes sont défavorisées dans leur capacité d'innovation par rapport à leurs concurrents américains ou asiatiques, à cause du cadre réglementaire qui est beaucoup plus strict ?

[Professor in innovation]
De nouveau, beaucoup plus strict, il faut être un peu plus nuancé. Aux Etats-Unis, il y a moins de règles, mais les règles sont beaucoup plus strictement enforced. Il y a des aspects pour lesquels c'est beaucoup plus contraignant qu'ici.

Il y a un peu cet idéalisme de dire, aux Etats-Unis, on fait ce qu'on veut, en Europe, il y a plein de règles. Non, ça dépend des domaines. Il y a aussi des différences en termes d'enforcement.

Aux Etats-Unis, vous pouvez aller en prison. En Europe, avant que quelqu'un… Regardez le scandale de Volkswagen avec les choses.

Ce n'est pas aussi simple que ça. En Chine, c'est encore différent. Il y a des règles très strictes, mais si vous avez le bon support, vous pouvez faire en sorte que la règle vous aide.

La Chine est un bon exemple. C'est l'opposé du libéralisme, et pourtant, ils innovent très bien. Ça montre bien que ce n'est pas aussi simple que ça.

Je pense qu'ici, il y a un aspect sans doute culturel de se dire qu'en Europe, on va réfléchir d'abord avant d'agir. De nouveau, en caricaturant. Il y a une tolérance pour l'expérimentation qui est sans doute moins forte en Europe qu'aux Etats-Unis.

En tout cas, que certains endroits aux Etats-Unis, certaines régions. Je pense aussi qu'on parle des Etats-Unis, mais non, ce n'est pas les Etats-Unis. C'est certains Etats ou certains endroits où ils sont prêts à encourager l'expérimentation, etc.

Et en Chine, même chose. Si le ministre Intel a dit que c'est bon, on y va. Si on prend par exemple les taxis autonomes, il y a déjà des expérimentations aux Etats-Unis, des expérimentations en Chine.

Il n'y en a pas en Europe. Parce que la capacité à autoriser ce type d'expérimentation est moins grande. Donc ça, c'est un premier élément.

Le deuxième élément, c'est la fragmentation dont on parlait tantôt. Si je suis ChatGPT, j'ai un interlocuteur, qui est le gouvernement fédéral, pour la plupart des choses. Il y a des choses qui sont définies au niveau des Etats, mais globalement, c'est quand même ça.

Si lui, c'est bon, c'est bon. En Chine, même chose. En Europe, j'ai l'Europe qui a 27 pays, puis j'ai encore les 27 pays, puis j'ai encore les régions, etc.

Clairement, pour moi, on revient sur l'argument d'hier. Sur la version risque, il faut être prudent et nuancé, parce que c'est un peu un cliché. Mais en tout cas, je la transformerais en sur la capacité à créer des espaces d'expérimentation, qui est sans doute plus importante aux Etats-Unis et en Chine qu'en Europe.

Il y a aussi des endroits aux Etats-Unis où les gens sont encore plus conservateurs qu'en Europe. C'est pour ça qu'il faut être plus nuancé. Il y a des espaces d'expérimentation plus présents aux Etats-Unis et en Chine pour des raisons très différentes.

Mais il y a aussi la fragmentation des marchés. Pour moi, ça, c'est l'argumentation principale.

[Quentin Roland]
Est-ce que le cumul des réglementations, et là, je comprends aussi le DSA et le AI Act, en plus du DMA et du GDPR, en Europe, crée-t-il un environnement trop rigide pour certains types d'innovateurs ?

[Professor in innovation]
Sans doute que le cumul crée de la complexité, on en a parlé tout à l'heure. Mais non, trop rigide, je ne sais pas vous dire, parce que ça dépend du point de vue de qui. Donc ça, je n'ai pas d'avis.

[Quentin Roland]
À l'inverse, pensez-vous que la réputation de l'Europe comme leader en régulation éthique peut devenir un avantage stratégique, fiabilité, confiance, exportabilité des standards ?

[Professor in innovation]
Je pense que c'est un peu aussi un cliché. Les Etats-Unis inventent, les autres entreprennent, l'Europe régule. C'est très à la mode de râler là-dessus.

Donc c'est un peu un cliché. Je pense que c'est un peu l'avenir nous le dira. C'est clair que quand vous anticipez un problème, et puis que le problème arrive, vous vous dites, ah, j'ai bien fait d'anticiper.

Si le problème n'arrive pas, les autres ont été plus malins. C'est comme la réglementation sur les effets sur la santé des téléphones mobiles. Si tout d'un coup, on avait découvert que ça donnait le cancer, certains vous auraient dit, ah, je vous l'avais bien dit.

Comme pour le moment, on n'a rien découvert, ce qui ne veut pas dire qu'il n'y en a pas. Mais en tout cas, on n'a pas découvert. Les autres vous disent, ah, je vous l'avais bien dit.

Je pense que c'est de nouveau un choix politique. Et on peut sans doute trouver des exemples dans les deux sens. Des exemples où le fait d'avoir été trop prudent a causé un problème.

Dans d'autres cas, on peut dire quelque chose, heureusement qu'on était prudent. Et de nouveau, ce n'est pas toujours dans le même sens. Il y a un cas d'école qui est la thalidomine.

On n'en voit plus beaucoup maintenant, heureusement. Mais c'était les gens qui avaient des tout petits bras, des toutes petites jambes. Et en fait, c'était un médicament qu'on donnait aux femmes enceintes pour contrer le malaise.

Et ce médicament a été interdit aux Etats-Unis 20 ans avant qu'il soit interdit en Europe. Parce qu'on a dit, attention, il y a un danger. Et là, 20 ans après, on s'est dit, on a bien fait d'interdire.

Et en Europe, on s'est dit, zut. Mais vous pouvez trouver le contraire. L'asbest, l'amiante est encore autorisée au Canada.

Pourquoi? Parce que c'est un des plus grands producteurs d'amiante au monde. Donc, on peut trouver des cas dans les deux sens où l'excès de prudence.

Est-ce que la prudence est une bonne chose? C'est après l'avoir réalisé qu'on s'en rend compte.

[Quentin Roland]
Tout à fait. Mon quatrième point est sur les logiques d'apprentissage stratégique dans un cadre contraint.

[Professor in innovation]
Juste, j'ai un autre ennemi, donc on va devoir un peu accélérer.

[Quentin Roland]
Certains professeurs, dont mon promoteur, évoquent l'idée de lancer un produit en Europe dans un contexte très réglementé. Ça peut permettre à une entreprise de mieux s'exporter ensuite vers d'autres régions. Cette stratégie d'apprentissage sous contrainte ressemble-t-elle pertinente?

[Professor in innovation]
Oui, c'est un peu ce qui peut le mieux, peut le moins. C'est l'exemple, c'est l'argument principal pour le développement des aspects environnementaux. C'est de dire et on voit, par exemple, il y a ça aujourd'hui dans la réglementation alimentaire aux Etats-Unis.

Suite au monsieur un peu original qu'ils ont mis à la tête du département de la santé. Ils veulent interdire toute une série d'additifs et de colorants qui sont interdits depuis longtemps en Europe. Et là, les entreprises européennes qui exportent aux Etats-Unis se disent qu'en fait, nous, on est déjà prêt.

Ça, on sait déjà faire. Donc, de nouveau, si vous avez anticipé, si ça se réalise. Mais si, par contre, ça ne se réalise jamais, ça ne sert à rien.

Donc oui, ça peut certainement être un argument.

[Quentin Roland]
Quels arbitrages stratégiques voyez-vous dans le choix entre conformité maximale et agilité innovante pour une start-up ?

[Professor in innovation]
Ça, je n'ai pas vraiment de réponse universelle. Je pense que peut-être l'argument, c'est les deux arguments sont par rapport à la prise de risque et par rapport aux attentes des clients du marché ciblé. Et c'est ça, à mon avis, qui devrait vous permettre de choisir.

[Quentin Roland]
Ok. Peut-on imaginer que les régulations deviennent des leviers d'innovation collaborative entre entreprises ? Interopérabilité, standards ouverts, éco-innovation ?

[Professor in innovation]
Oui, là, on revient sur le fait de développer un cadre, un terrain de jeu, un cadre clair. Ça facilite les collaborations. Ok.

[Quentin Roland]
Maintenant, on vient en conclusion. Avez-vous en tête des exemples concrets d'entreprises qui ont pu transformer ces contraintes réglementaires en leviers d'innovation ?

[Professor in innovation]
Dans le domaine de la privacy, il y a une série de gens qui essaient de se positionner comme super safe, comme souverain, etc. Et donc, ça, ce sont des exemples. Est-ce qu'il y a des exemples de réussite ou pas, ça, je ne sais pas.

Peut-être qu'on pourrait citer la boîte qui fait de la data governance, Colibra. Est-ce que Colibra voit son succès à ça ? Je ne sais pas.

Mais en tout cas, la réglementation a mis la pression sur les entreprises à mieux maîtriser et comprendre ce qu'ils faisaient avec les données. Et donc, dans ce contexte, à mieux

sensibiliser les entreprises à ça. Et donc, si vous venez avec une solution de data governance, vous dites, mais moi, je vais pouvoir vous aider à dire quelles données vont où, par qui, etc.

On peut argumenter qu'en tout cas, ça leur a été favorable.

[Quentin Roland]
Et enfin, ma dernière question, quel conseil stratégique donneriez-vous à une PME numérique européenne qui souhaite innover tout en restant conforme aux exigences européennes ?

[Professor in innovation]
D'aller en B2B parce que B2C est mort. Enfin, ce n'est pas mort, mais la place est prise. Je pense qu'en B2C, les acteurs américains et chinois ont bénéficié de leur taille et du fait qu'en Europe, ils ne sont pas trop inquiétés de la compliance pour avoir un avantage concurrentiel qui va être difficile à répliquer.

Par contre, dans le domaine des données liées aux entreprises, il y a encore énormément d'espace à prendre. En ce sens qu'il n'y a pas aujourd'hui un acteur qui a mis la main sur toutes ces données et qui peut faire mieux que tout le monde. Alors que vous combinez Google, Meta et quelques acteurs chinois, les données sur les personnes individuelles privées, ils ont déjà accumulé un nombre de données et un savoir extrêmement important.

Le deuxième conseil serait d'être beaucoup plus je vais parler de strategic data asset, d'être beaucoup plus conscient et sensibilisé de dire quelles sont les données qu'on a ou qu'on pourrait avoir. Et quelles sont les données qu'on devrait avoir. Si je n'ai pas le contrôle de ces données-là, je suis out of business. C'est l'exemple de la bataille pour l'ADAS.

L'ADAS, c'est le GPS de la voiture. C'est la partie un peu intelligente. Les constructeurs automobiles en particulier allemands se sont dit qu'on ne pouvait pas laisser ça à Google ou à Apple.

Si demain tout est sous contrôle via le smartphone, je ne vends plus que de l'acier, des roues, une batterie et toute la valeur ajoutée. Je dois absolument ne pas perdre la main sur les données de mes utilisateurs et de mes clients. Les stratégiques d'ADAS, c'est pour moi un enjeu.

C'était une question qui n'était pas partie de la réflexion de ces entreprises.

[Quentin Roland]
Merci beaucoup, c'était très intéressant et ça m'a aidé à rédiger mon mémoire.

[Professor in innovation]
Bonne continuation.

[Quentin Roland]
Merci, à vous aussi. Au revoir.

Appendix C.5: Interview transcript with Nicolas Parvais, Security Manager at Elium (knowledge management start-up)

[Quentin Roland]
Bonjour, dans le cadre de mon mémoire de Master 2 à l'UCLouvain (Louvain School of Management), je m'intéresse aux effets conjoints du RGPD et du DMA sur les entreprises européennes du numérique. Je souhaite comprendre comment ces cadres influencent concrètement les modèles économiques, les stratégies d'innovation et les arbitrages réglementaires, notamment pour les start-ups technologiques actives dans des domaines comme la gestion de la connaissance, l'IA ou le SaaS collaboratif.
Mon premier thème étant la conformité et gouvernance des données. Le RGPD a-t-il modifié votre manière de concevoir ou de structurer vos solutions de knowledge management (par exemple : droits d'accès, stockage, logs, données sensibles) ?

[Nicolas Parvais]
Le RGPD n'a pas fondamentalement transformé notre manière de concevoir ou de structurer notre solution de knowledge management, dans la mesure où la protection des données, la sécurité et la confidentialité faisaient déjà partie intégrante de notre approche. Nous avions mis en place, dès l'origine, des mesures techniques et organisationnelles robustes pour garantir un haut niveau de sécurité : gestion fine des droits d'accès, journalisation des actions (logs), chiffrement, ainsi qu'un contrôle strict sur le stockage et le traitement des données sensibles.
Toutefois, l'entrée en vigueur du RGPD a renforcé certaines exigences et nous a amenés à formaliser davantage nos pratiques. Par exemple, nous avons revu et documenté nos procédures internes pour assurer la traçabilité des traitements, la limitation des accès au strict nécessaire (principe du moindre privilège), et la gestion des durées de conservation des données. Le RGPD a également encouragé une approche encore plus rigoureuse en matière de transparence vis-à-vis des utilisateurs et de documentation des choix techniques, en particulier en ce qui concerne la protection dès la conception et par défaut (privacy by design & by default). En résumé, si le RGPD n'a pas bouleversé notre démarche, il a été un levier utile pour renforcer, cadrer et valoriser des principes que nous appliquions déjà dans le développement et le déploiement de notre solution.

[Quentin Roland]
Avez-vous mis en place une politique spécifique de privacy by design dans vos cycles de développement produit ?

[Nicolas Parvais]

Oui, les développements de notre produit respectaient déjà le modèle de "Privacy by Design".

[Quentin Roland]
Quelles ont été les principales contraintes ou difficultés rencontrées pour atteindre (ou maintenir) la conformité RGPD en tant que start-up ?

[Nicolas Parvais]

En tant que start-up développant une solution SaaS, l'une des principales contraintes liées à la conformité RGPD réside dans notre dépendance à l'égard de services tiers, souvent indispensables à notre agilité technologique. Cette dépendance est parfois perçue comme problématique par certains clients, notamment en ce qui concerne le traitement des données par des prestataires situés hors de l'Union européenne, même lorsque ceux-ci respectent les exigences du RGPD. Cela s'est notamment manifesté autour des questions d'hébergement.

Pour répondre à ces préoccupations, nous avons dû adapter notre architecture technique et proposer des options spécifiques. Par exemple, nous avons intégré dans notre offre une solution d'hébergement en France, reposant sur une infrastructure certifiée SecNumCloud, afin de répondre aux exigences de souveraineté exprimées par certains clients. Ce type de contrainte ne découle pas directement du RGPD, mais il a été largement renforcé par les sensibilités et attentes accrues qu'a suscité la mise en œuvre du règlement.

Par ailleurs, la RGPD impose, en tant que sous-traitant, d'informer les clients de tout changement concernant les sous-traitants ultérieurs (services tiers). Dans le cadre d'une solution SaaS multi-tenant, il est matériellement impossible de recueillir l'accord préalable de chaque client pour chaque évolution technique, notamment lors du remplacement ou de l'ajout d'un prestataire. Nous avons donc dû adapter nos conditions contractuelles pour intégrer une clause prévoyant une information préalable des clients dans un délai raisonnable (généralement quelques jours). Si un client refuse le recours au nouveau prestataire, il dispose alors de la possibilité de résilier son contrat. Cette approche, bien que contraignante, reste conforme au cadre légal et nous permet de maintenir un équilibre entre conformité réglementaire, transparence et agilité opérationnelle.

[Quentin Roland]

Avez-vous ressenti un impact sur la relation client ou la stratégie commerciale à cause du RGPD (ex. : clauses contractuelles, réassurance, exportabilité) ?

[Nicolas Parvais]

Oui, le RGPD a eu un impact significatif sur la relation client et, par extension, sur notre stratégie commerciale. L'un des changements les plus marquants concerne les attentes accrues de nos clients en matière de transparence sur le traitement des données, et en particulier sur l'implication de prestataires tiers. Là où, avant le RGPD, peu de clients s'intéressaient à la localisation des données ou à la nature des services sous-jacents, nous constatons désormais une vigilance systématique sur ces points.
En particulier, une majorité de nos clients expriment une exigence forte : que leurs données ne soient pas traitées ou hébergées par des sociétés non européennes, et qu'elles restent stockées dans des centres de données situés exclusivement en Europe. Cette contrainte nous a conduits à renforcer considérablement notre communication autour de notre chaîne de sous-traitance technique. Nous avons intégré dans notre démarche commerciale, dès la phase de prospection, une documentation détaillée sur l'ensemble des services tiers que nous utilisons, leur rôle, leur localisation, ainsi que les garanties qu'ils offrent en matière de conformité RGPD.
De plus, des évolutions contractuelles ont été nécessaires. Nous avons adapté nos conditions générales et nos contrats clients pour intégrer des clauses spécifiques liées au RGPD : obligations d'information, conditions d'exportabilité des données, gestion des sous-traitants ultérieurs, etc. Dans certains cas, des clients exigent même une clause d'approbation préalable pour tout ajout ou remplacement de prestataire technique, ce qui nécessite un dialogue constant et une anticipation des impacts juridiques et opérationnels.
En résumé, le RGPD a introduit une nouvelle dimension dans notre relation client, fondée sur la transparence, la réassurance et la capacité à démontrer concrètement notre conformité. Cela a renforcé la confiance dans nos offres, mais a aussi nécessité un investissement conséquent en documentation, en contractualisation et en gestion des attentes.

[Quentin Roland]

Mon deuxième thème est l'innovation produit et arbitrages technologiques. Est-ce que certaines fonctionnalités ont été modifiées, ralenties ou évitées pour des raisons de conformité ou de prudence vis-à-vis des régulations ?
[Nicolas Parvais]

Oui, certaines fonctionnalités ont été ajustées, retardées ou écartées en raison de considérations liées à la conformité RGPD ou par souci de prudence réglementaire. L'un des principaux axes d'attention a concerné le choix de nos prestataires techniques. Nous avons volontairement orienté notre stratégie vers l'usage exclusif de services tiers situés en Europe, ce qui a parfois limité notre marge de manœuvre fonctionnelle ou imposé des adaptations techniques pour garantir la compatibilité avec ces prestataires. Ce choix, bien qu'exigeant, nous a permis d'apporter une réponse claire et conforme aux attentes réglementaires, mais aussi aux exigences de certains clients en matière de souveraineté des données.
Par ailleurs, nous avons intégré des fonctionnalités spécifiques dans notre solution pour permettre aux utilisateurs d'exercer facilement leurs droits en vertu du RGPD (accès, rectification, suppression, portabilité, etc.). Cela a nécessité une réflexion approfondie sur la structuration des données, leur traçabilité, ainsi que sur les interfaces utilisateur.
Enfin, nous avons mis en place un mécanisme de feature flags, qui permet d'activer ou de désactiver dynamiquement certaines fonctionnalités selon les préférences et les contraintes contractuelles des clients. Cette approche nous permet de gérer finement l'exposition des données à certains services tiers, en particulier lorsque ces derniers interviennent dans des fonctionnalités avancées. Ainsi, certaines fonctionnalités peuvent être déployées de manière différenciée, voire ne jamais être activées pour certains clients si cela va à l'encontre de leur politique de traitement des données.
Ce dispositif nous offre une flexibilité précieuse, tout en respectant les principes de protection des données dès la conception (privacy by design) et par défaut (privacy by default), comme le requiert le RGPD.
[Quentin Roland]
À l'inverse, diriez-vous que la contrainte réglementaire a favorisé certains choix d'architecture ou de différenciation produit (par exemple en matière de sécurité, traçabilité ou transparence) ?

[Nicolas Parvais]

Oui, nous pouvons dire que les exigences du RGPD ont agi comme un catalyseur positif sur certains choix d'architecture technique et sur notre positionnement produit. En intégrant nativement des mécanismes permettant aux utilisateurs d'exercer leurs droits (accès, suppression, portabilité, etc.), nous avons renforcé la transparence et la traçabilité au sein de notre solution. Ces fonctionnalités, initialement développées pour répondre à des obligations légales, se sont révélées être des éléments différenciateurs forts, en particulier dans des environnements où la confiance et la maîtrise des données sont des critères de sélection majeurs.
Par ailleurs, notre choix stratégique de privilégier des services tiers situés en Europe, souvent perçus comme plus conformes et plus respectueux des exigences de souveraineté numérique, a contribué à asseoir notre crédibilité auprès de clients sensibles à ces enjeux, notamment dans les secteurs public et parapublic, ou dans les industries réglementées. Cela a renforcé notre proposition de valeur face à des concurrents dont les solutions reposent sur des infrastructures non européennes.
Enfin, cette contrainte réglementaire a eu pour effet d'orienter notre architecture vers une plus grande modularité, avec une attention accrue portée à la traçabilité des traitements, à la gestion des logs, et à la sécurité des flux. Ce sont aujourd'hui des atouts que nous mettons en avant dans nos démarches commerciales, et qui participent à créer un climat de confiance durable avec nos clients.

[Quentin Roland]
La conformité RGPD est-elle perçue en interne comme une valeur ajoutée ou plutôt comme un frein à la scalabilité ?
[Nicolas Parvais]

En interne, la conformité RGPD est parfois perçue comme un frein, notamment lorsqu'on la compare à la flexibilité dont peuvent bénéficier certains concurrents non soumis aux mêmes exigences réglementaires, notamment en dehors de l'Union européenne. Cette perception s'explique par les contraintes supplémentaires qu'elle impose à différents

niveaux de l'organisation : dans les choix technologiques, dans les processus internes, mais également dans le design fonctionnel de notre solution.
Par exemple, certaines fonctionnalités que nous aurions pu développer rapidement en intégrant des services tiers non européens ont nécessité une évaluation rigoureuse au regard des principes du RGPD, voire ont dû être réorientées vers des alternatives plus conformes mais parfois moins matures ou plus coûteuses. Ce processus ralentit potentiellement la mise en œuvre de certaines évolutions produit, et peut complexifier notre stratégie de montée en charge (scalabilité), en particulier lorsqu'il s'agit de standardiser l'architecture pour tous les clients.
Cela dit, cette rigueur réglementaire nous oblige aussi à adopter une approche plus structurée et pérenne, qui, à moyen terme, peut devenir un avantage en matière de confiance, de solidité technique, et de positionnement sur des marchés sensibles aux enjeux de conformité. Mais il est vrai que sur le court terme, le RGPD est vécu comme un facteur de ralentissement dans notre capacité à innover ou à intégrer rapidement certaines solutions technologiques.

[Quentin Roland]
Mon troisième thème est le positionnement stratégique et la concurrence. Pensez-vous que les entreprises européennes comme Elium sont désavantagées par rapport à des concurrents non européens qui opèrent avec des obligations réglementaires plus souples ?
[Nicolas Parvais]
Il est indéniable que les entreprises européennes peuvent être désavantagées sur certains plans par rapport à leurs concurrents non européens, en particulier en ce qui concerne la rapidité d'exécution, la flexibilité technologique et la capacité à intégrer certains services tiers plus facilement accessibles hors du cadre strict du RGPD. Le niveau d'exigence imposé aux entreprises opérant en Europe est élevé, notamment en matière de documentation, de traçabilité, de limitation des traitements, ou encore de gestion des sous-traitants. Ces obligations peuvent générer des coûts supplémentaires, allonger les cycles de développement, et freiner l'innovation à court terme.
Cela dit, il est important de rappeler que toute entreprise, européenne ou non, est tenue

de respecter le RGPD dès lors qu'elle traite des données personnelles de citoyens européens. Dans ce contexte, la conformité devient un enjeu commercial majeur : les clients européens sont de plus en plus attentifs à la localisation des données, à la souveraineté numérique, et aux garanties offertes par leurs prestataires. Cela peut rééquilibrer partiellement la situation en faveur d'acteurs européens qui intègrent dès le départ la conformité RGPD comme un avantage compétitif et non uniquement comme une contrainte.

En ce sens, bien que les entreprises européennes soient soumises à un cadre réglementaire strict, elles peuvent tirer parti de cette exigence en capitalisant sur la transparence, la sécurité, et la fiabilité de leurs services, des valeurs de plus en plus recherchées, notamment dans les secteurs publics, réglementés ou sensibles.

[Quentin Roland]

Le DMA s'adresse surtout à des grandes plateformes, mais pensez-vous qu'il pourrait avoir un impact indirect sur des acteurs B2B comme vous (interopérabilité, accès au marché, exposition aux grandes plateformes) ?

[Nicolas Parvais]

Bien que le Digital Markets Act (DMA) cible principalement les grandes plateformes numériques, il est probable que ses effets aient un impact indirect sur des acteurs B2B comme nous. En effet, même si notre solution n'est pas directement concernée par ce règlement, les décisions stratégiques de nos clients peuvent être influencées par les conséquences du DMA sur leur propre écosystème digital.

Par exemple, nos clients, qui collaborent avec de grandes plateformes régulées par le DMA, évaluent l'impact potentiel de cette réglementation sur leur capacité d'interopérabilité, leur accès au marché, et leurs interactions avec ces acteurs majeurs. Ce contexte réglementaire modifie donc leur perception et leurs priorités, ce qui peut à son tour influencer leurs exigences vis-à-vis de nos services, ainsi que leurs décisions d'investissement et d'intégration.

Ainsi, même indirectement, le DMA contribue à redéfinir l'environnement concurrentiel et stratégique dans lequel nous évoluons, ce qui nous incite à rester attentifs à ces évolutions pour adapter notre offre et notre positionnement en conséquence.

[Quentin Roland]
Avez-vous observé une différence dans les attentes réglementaires ou les perceptions clientes entre vos marchés belges, européens ou extra-européens ?
[Nicolas Parvais]

Effectivement, nous observons des différences marquées dans les attentes réglementaires et les perceptions des clients selon les marchés. Sur le marché européen, et particulièrement en France, la sensibilité à la réglementation européenne, notamment au RGPD, est très élevée. Nos clients français, en particulier les grandes entreprises, accordent une importance particulière à la souveraineté de leurs données ainsi qu'au strict respect des obligations réglementaires. Ils exigent des garanties fortes sur la localisation des données, la sécurité des traitements, ainsi que sur la conformité des sous-traitants impliqués.
En revanche, cette vigilance est moins prononcée chez nos clients extra-européens, pour lesquels les préoccupations liées à la réglementation européenne sont souvent perçues comme moins prioritaires ou moins contraignantes, sauf dans la mesure où ils interagissent avec des données ou partenaires européens.
Sur le marché belge, la sensibilité est généralement intermédiaire, reflétant une culture réglementaire européenne mais avec parfois une approche un peu plus pragmatique selon les secteurs d'activité.
Ces différences nous obligent à adapter notre discours commercial, notre documentation et nos offres selon les marchés, afin de répondre au mieux aux attentes spécifiques de chaque clientèle.
[Quentin Roland]
Mon quatrième thème est en rapport avec les perspectives et rôle de la régulation. Pensez-vous que le cadre réglementaire européen actuel favorise ou freine l'émergence d'acteurs européens crédibles à l'international ?
[Nicolas Parvais]
Le cadre réglementaire européen actuel, avec ses exigences strictes en matière de protection des données et de conformité, peut effectivement représenter un frein à l'émergence rapide et à l'expansion internationale des acteurs européens. Ces restrictions

imposent des contraintes techniques, organisationnelles et financières importantes, qui peuvent limiter la capacité des entreprises à innover ou à déployer rapidement des solutions compétitives à l'échelle mondiale.
Cependant, ce même cadre réglementaire constitue également un gage de sérieux et de fiabilité sur le marché européen. Les entreprises capables de développer des solutions pleinement conformes au RGPD et aux autres normes européennes bénéficient d'un avantage certain dans leur région, en répondant aux attentes croissantes des clients en matière de sécurité, de transparence et de souveraineté des données.
En résumé, bien que la réglementation européenne puisse freiner la rapidité de croissance et l'agilité des acteurs locaux face à des concurrents étrangers plus flexibles, elle crée également une base solide et différenciante, qui favorise la crédibilité et la confiance sur le marché intérieur européen. L'enjeu pour les entreprises européennes est donc de tirer parti de ce cadre pour construire une proposition de valeur unique tout en cherchant à optimiser leur compétitivité à l'international.

[Quentin Roland]
Votre stratégie de développement a-t-elle été pensée pour répondre d'abord aux contraintes européennes, avant d'être exportée ailleurs ?

[Nicolas Parvais]

Absolument. En tant qu'entreprise européenne, notre stratégie de développement a été conçue en priorité pour répondre aux exigences et contraintes spécifiques du cadre réglementaire européen, notamment celles liées au RGPD. Cette approche nous permet de garantir à nos clients une conformité robuste et une maîtrise complète des exigences légales dès le départ.
En ciblant d'abord le marché européen, nous assurons une base solide et fiable pour notre solution, ce qui facilite ensuite son adaptation et son déploiement progressif sur d'autres marchés internationaux. Cette méthodologie "conformité d'abord" est un élément clé de notre stratégie commerciale et technique, et contribue à renforcer la confiance de nos clients tout en préparant l'export de notre solution dans un contexte réglementaire mondial plus varié.

[Quentin Roland]
Quel type d'évolution réglementaire souhaiteriez-vous voir à l'avenir pour que la régulation accompagne l'innovation plutôt que la freiner ?
[Nicolas Parvais]

Je n'ai pas de réponse.

[Quentin Roland]
Pour conclure, quels conseils donneriez-vous à une start-up numérique européenne qui débute aujourd'hui et doit composer dès le départ avec le RGPD, le DMA et potentiellement le DSA ?
[Nicolas Parvais]

Je conseillerais à toute start-up numérique européenne débutant aujourd'hui d'intégrer les exigences réglementaires telles que le RGPD, le DMA et potentiellement le DSA dès la phase de conception de leur modèle d'affaires et de leur produit. Ces réglementations ne doivent pas être perçues uniquement comme des contraintes, mais aussi comme des éléments stratégiques qui orienteront leurs choix technologiques, commerciaux et organisationnels.
Il est essentiel de définir dès le départ le marché cible, européen ou international, afin d'adapter la conformité en conséquence. Se conformer aux réglementations européennes implique un investissement en temps, en ressources et en coûts, qu'il faut anticiper dans la planification financière et opérationnelle. Cela passe par la mise en place d'une gouvernance des données rigoureuse, la sécurisation des traitements, la documentation précise des processus, ainsi qu'une transparence totale vis-à-vis des clients et partenaires.
En résumé, mieux vaut considérer la conformité réglementaire comme un socle sur lequel bâtir une relation de confiance avec ses clients et partenaires, un levier différenciant plutôt qu'un simple frein. Cette approche proactive facilitera non seulement la croissance durable de la start-up, mais aussi son accès aux marchés européens et internationaux.

[Quentin Roland]

Avez-vous le sentiment que les régulateurs ou institutions européennes écoutent suffisamment les start-ups dans la définition des cadres législatifs ?

[Nicolas Parvais]

À mon sens, les start-ups européennes ne sont pas suffisamment écoutées dans le processus de définition des cadres législatifs par les régulateurs et institutions européennes. Sur la scène internationale, de nombreuses start-ups européennes se retrouvent désavantagées face à leurs concurrents extra-européens, qui peuvent proposer des solutions technologiquement similaires, mais sans être soumis aux mêmes contraintes légales strictes imposées par l'Europe.

Même si l'objectif principal de ces réglementations est légitime, protéger les individus et leur vie privée, il semble que l'attention soit davantage portée sur les grandes plateformes et mastodontes américains, qui traitent effectivement un volume massif de données personnelles. Paradoxalement, les petites entreprises et start-ups, qui traitent parfois moins d'informations sensibles, se retrouvent soumises aux mêmes obligations, ce qui engendre une contrainte budgétaire importante. Cette situation peut ralentir, voire freiner, leur capacité à innover et à se développer, alors même qu'elles jouent un rôle crucial dans l'écosystème numérique européen.

Il serait donc pertinent que les législateurs prennent davantage en compte la réalité et les spécificités des start-ups afin d'instaurer un cadre plus adapté, équilibrant protection des données et soutien à l'innovation.

[Quentin Roland]

Merci beaucoup pour votre temps, aurevoir.

Abstract:

This thesis explores the evolving interaction between two cornerstone EU regulations: the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA), and their combined impact on digital business models and innovation within the European Union. Adopting a qualitative and exploratory methodology, the research is based on expert interviews with regulators, legal scholars, startup founders, and corporate professionals. It analyses how European firms adapt to these regulations depending on their strategic posture as regulatory takers or shapers, and evaluates the trade-offs experienced by various stakeholders including large platforms, SMEs, consumers, and policymakers.

The results show that the GDPR's focus on privacy and the DMA's focus on market fairness and contestability can work together and against each other. Each rule encourages user empowerment and competitive dynamics on their own, but when they are put into effect together, they still have problems with enforcement that isn't consistent and governance that isn't connected. Case studies show how these rules hinder the ability to innovate, especially for European companies trying to compete with non-EU IT giants.
In the end, this study raises the question of whether the existing regulatory framework really makes things better for consumers and gives European digital markets a long-term competitive edge.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Louvain School of Management
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique
www.uclouvain.be/lsm