

UNPACKING CURRENT DEVELOPMENTS IN THE INFORMATION SPACE



“It is essential to defend the GDPR not only as a legal framework, but as a genuine political and democratic project.”

Suzanne Vergnolle,
Associate Professor,
Conservatoire National des Arts et Métiers (CNAM)

In May 2025, the European Commission adopted a proposal to reopen and simplify the founding text of personal data protection in the European Union, the General Data Protection Regulation (GDPR). The rationale behind this move is the burden placed on small and medium-sized enterprises (SMEs) to maintain records of collected data. Meanwhile, civil society organizations such as European Digital Rights (EDRI), are warning that “reopening the GDPR is a threat to rights, accountability and the future of EU digital policy”.

Katharina Zuegel, the Forum’s Policy Director, spoke with Dr. Suzanne Vergnolle, Associate Professor in Technology Law at the Cnam (Conservatoire national des arts et métiers). They discussed the significance of the GDPR in safeguarding the rights of European citizens, its potential impact across a wide range of sectors, and the broader global context in which this reopening is occurring, and must be taken into account.

Could you please introduce yourself and explain your area of expertise?

My name is Suzanne Vergnolle, and I am an Associate Technology in Digital Law at the Cnam (Conservatoire national des arts et métiers). I hold a PhD in Private Law from Paris Panthéon-Assas University. My doctoral research focused on **the effectiveness of protecting individual’s rights by data protection law**. The aim was to analyze this legal framework, particularly the GDPR and France’s Data Protection Act (Loi Informatique et Libertés), to assess the extent to which these texts truly deliver on the guarantees and protections they promise.

My research falls within the field of technology law. I focus initially on personal data protection, but extended my research to the regulation of online platform activities, particularly in relation to **new regulations** such as the Digital Services Act (DSA) and broader European data governance rules.

Before we begin, could you define what personal data is?

Personal data is any information relating to an identified or identifiable natural person. We often immediately think of things like a name, voice, or image, but it also includes a social security number, fingerprints, or health data, such as blood type, for example.

“Many people are unaware that their data is being collected and used, which makes this right essential.”

Turning to today’s topic, what exactly is the GDPR, and more importantly, how does it make a real difference for citizens? How does it protect them, and what rights does it grant?

The GDPR, or General Data Protection Regulation, is a European regulation adopted in 2016 and **entered into force in May 2018**. It applies across all EU Member States. The core idea behind this text is **to provide guarantees and transparency in the processing of personal data**.

One of the most important rights it establishes is the **right of access**, meaning the right to know whether data about us is being processed, and for what purposes. Many people are unaware that their data is being collected and used, which makes this right essential.

There is also the **right to rectification**: if a piece of data is incorrect, the data subject can request that it be corrected. This right is particularly important in sectors like banking. For example, an error in a loan repayment history can skew the calculation of an interest rate. Being able to correct this information can have very concrete and significant consequences.

The GDPR also establishes other rights, such as **data portability**, the ability to transfer your data to another service, and the right to erasure (also known as the “right to be forgotten”).

It’s also a regulation that **promotes competition**, by establishing a common framework and prohibiting uncontrolled data processing. It aims to level the playing field for all actors when it comes to respecting fundamental rights.

You’ve already mentioned health and the banking sector as areas affected by this regulation. What are some other sectors where the GDPR has a significant impact, even if citizens aren’t always aware of it?

One of the specific features of the GDPR is that it applies extremely broadly, it affects both small organizations and large companies, as well as the public and **affects both**

private sectors. It's a **cross-cutting regulation**, applying to virtually every field of activity.

Beyond **health** and **finance**, the GDPR plays an important role in other areas too, such as **human resources**, particularly during recruitment processes; **social media platforms**, which are frequently subject to sanctions by data protection authorities; **insurance companies and health insurance**, which must comply with strict rules regarding health data; but also the **education sector**, and **media**.

As soon as there is any processing of personal data, and the definition of personal data is very broad, the GDPR applies. Because the definition of personal data is broad, **the regulation, in practice, affects all individuals and nearly every organization.**

“The GDPR is a regulation that, in practice, affects all citizens and nearly every organization.”

Going back to social media and digital platforms more broadly, in practical terms, what differences do European citizens experience compared to those in countries that don't have a regulation equivalent to the GDPR?

A few years ago, Facebook launched a **facial recognition system for photos** shared on its platform. However, this type of technology could not be rolled out in the same way in Europe as it was in the United States. The same goes for **contact mapping**: because European rules are more restrictive, certain types of data processing are simply not permitted. These are concrete examples of how application differs across regions.

Another interesting point concerns **data breaches**. In Europe, there is a clear obligation to notify the data protection authority in the event of a security incident. And if the breach poses a significant risk to the rights and freedoms of individuals, the people affected must also be informed. A recent example of this was the **leak of personal data belonging to subscribers of Free** (1), who were quickly notified so they could protect themselves against phishing attempts.

Let's stay with the topic of social media and the information space. To what extent does European regulation protect us from the use of our data for targeted advertising, or from the exploitation of new artificial intelligence tools?

This brings us to an important distinction between the theory, what the legal texts provide for, and practice, meaning how they're actually implemented and enforced. What we're seeing is that **there are sometimes diverging interpretations of the**

(1) Internet and phone provider.

GDPR, both among experts; data protection authorities and also jurisdictions. Not all of them interpret the regulation the same way.

Taking a recent example: the Irish Data Protection Authority has just allowed Facebook to use data shared by adult users in Europe to train its artificial intelligence (AI) systems. Yet, some experts have a very different reading of the GDPR on this issue.

When it comes to **targeted advertising**, we've also seen the **limits of the GDPR**. That's why another regulation was introduced to complement it: the **Digital Services Act (DSA)**, part of the EU's broader digital strategy.

This regulation sets specific rules, notably by banning targeted advertising directed at minors. It also **prohibits the use of sensitive data**, such as health, biometric, religious, political, or trade union-related data, **for ad targeting**. These are precisely the types of data most likely to be exploited to spread disinformation.

So we can see that **the GDPR and the DSA are complementary**. The DSA, which came into force in February 2024, addresses more recent challenges linked to the fast evolution of digital practices.

“Data protection addresses a crucial need, and in absence of a clear framework, the consequences can be harmful on a large scale.”

Right now, there is talk about reopening the GDPR and modifying certain rights. What risks would be associated with such a reform? Which rights could be threatened?

This is a very important question. To answer it, I think it's useful **to put the GDPR in its context**. We sometimes forget that this regulation didn't come out of nowhere. It builds on an earlier directive, Directive 95/46/EC, adopted in 1995 and gradually implemented in the Member States.

This directive imposed a **declaration system**: as soon as a file containing personal data was created, it had to be declared to the data protection authorities specifying which data was collected, for what purpose, how it would be processed, etc. Over time, many felt that these obligations represented a **heavy administrative burden** and didn't necessarily effectively address data protection challenges.

The approach therefore evolved with the GDPR: **we moved from a system of prior formalities to a logic of continuous compliance**, risk analysis, and justification of processing. And I believe this evolution was justified.

But today, **we are hearing similar arguments again**: some actors are once again asking for a **lightening of obligations**. What we actually observe is that these organizations tend to want to avoid applying the rules they are bound to.

And this poses a real problem because organizations that, for seven years, have

invested time, money, and resources to comply with the regulation today risk being penalized if the requirements are eased. This would send a very negative signal, as if the compliance efforts had been for nothing.

On the other hand, if adjustments are to be made, I think they should not be so much about the obligations of the entities concerned but about the way the GDPR is implemented and enforced. **There needs to be stronger harmonization of the interpretation** of the text by data protection authorities across different countries. The European Commission has actually begun working on this issue because we see significant disparities. As I mentioned earlier, the Irish authority is often criticized for its slow handling of Big Tech cases and for some of its interpretations, which are not always upheld by European bodies or courts.

So yes, there is room for improvement, but **this must be done without undermining the fundamental guarantees it offers.**

“There is room for improvement in the GDPR’s implementation, but this must be done without undermining the fundamental guarantees it offers.”

In what global context can we place the current debate about the GDPR?

This debate takes place within a broader context, what Anu Bradford theorized as the **“Brussels Effect”**. The idea is that some European regulations, like the GDPR, have an influence that goes beyond the borders of the EU because they inspire other countries to adopt similar standards.

Why? Because these rules result from a **complex balance between the views of 27 Member States and three institutions** (the European Commission, the Council, and the Parliament), each bringing a different perspective, and the resulting compromise **brings a common scope.**

In the case of the GDPR, this balance enabled the adoption of a fundamental text that protects citizens and which, through its impact, has inspired similar legislation in Asia, Africa, and Latin America. It must be said that **data protection addresses a crucial need, and in the absence of a clear framework, the consequences can be harmful on a large scale.**

“This text embodies deeply European, humanist, and in many ways universalist values.”

Why is the GDPR a key tool for strengthening a healthy media ecosystem and resilient democracies in Europe?

I believe the GDPR contributes to the **protection of journalistic sources**, in a way. It allows better management of sensitive data and information exchanged as part of journalistic work. It is a tool that **indirectly supports press freedom and transparency**, which are essential pillars of any democracy.

We spoke about the influence of the GDPR. But in the current context, where criticisms of regulation are multiplying, how can we explain this resurgence of the desire to deregulate?

What we observe today is a kind of **collective amnesia about the reasons that led to the adoption of the GDPR**. We must not forget that this regulation was adopted in the wake of **Edward Snowden's revelations**. At that time, we became aware of the extent of mass surveillance and its danger for individuals' privacy and democracy.

In response, Europe adopted the GDPR. And I believe that **the threats have not disappeared**, maybe even amplified. In fact, they have evolved: disinformation, fake news, deepfakes, and a whole range of new things made possible by artificial intelligence technologies, which make it even easier to manipulate people today.

And the GDPR, in a way, is a tool to fight against these abuses. It imposes obligations of transparency, information about data processing, and their purposes. These are safeguards against manipulation and losing control over our own data.

“It is essential to defend the GDPR not only as a legal framework but as a genuine political and democratic project.”

Current criticisms often ignore this dimension. They undervalue how **this text embodies deeply European, humanist, and in many ways universalist values**, especially at a time when our democracies are under pressure and influence. This is why it is essential to defend the GDPR not only as a legal framework but as a genuine political and democratic project.