The Rule of Law and Digital Surveillance, Personal Data, Privacy and Platform Regulation

-North Macedonia's path to EU Integration-

Author:
Evgenija Janakieska

Skopje, December 2025

This analysis argues that while the EU has developed an advanced legal framework to regulate digital surveillance and platforms, countries like North Macedonia face a structural gap between legal alignment and real power, turning the rule of law into a formal rather than lived protection.

Introduction and context: How our daily clicks turn into power and profit?

Digital surveillance enters spaces that feel intimate for people. Smart watches sit on our wrists. Recommendation feeds follow our eyes. AI systems read patterns in our movements and clicks. We order food from our phones. We chat with our friends, family, and colleagues on social media platforms. Each of our daily social interactions is now digitalised. Companies turn all this into profit.

Smart wearables give a good entry point for digital surveillance. Wang writes about the "quantified body" and shows how people use devices to track health and performance (Wang, 2025). The most used smart wearable is the smartwatch, which counts steps, monitors heart rate, tracks sleep, and provides fitness scores. Many users feel that this helps them set goals, see their progress, and change their habits. The device speaks the language of empowerment and self-care. It promises control.

Social media gives another clear entry point. Instagram, TikTok, Facebook, and every other social media platform "invite" people to post photos of intimate moments, share their opinions, and express their feelings about political topics, products, services, and more. The feed shows everything in one continuous stream: friends, influencers, news, ads, politics, makeup, culture, sponsored posts, memes, art—endless, spectacle-like. In this "spectacle," people scroll, people like, share, and comment on content. They feel connected and informed. They build a public image of themselves and a sense of belonging in this virtual society. The platform speaks the language of community and expression. It promises visibility and inclusion.

AI tools add another layer. Chatbots answer questions, write theses, help with work reports, check grammar, offer psychological counselling, read astrological charts, and prepare funny photo manipulations. In-app AI filters change your face—making your eyes pop, adding freckles, and making your waist tiny.

This policy brief was prepared under the project Building bridges for a common future: Rule of law in view of EU accession, funded by the European Union. The contents of this Brief do not reflect the official opinions and positions of the European Union. Responsibility for the information and views expressed in this Brief lies entirely with the European Policy Institute (EPI) - Skopje.

Moreover, platforms like Wolt, Temu, Uber, and similar services show how this logic permeates everyday consumption and work. Wolt connects people with restaurants and couriers. Temu sells a wide range of affordable products directly through its app. Users order food or goods with a few taps. They track deliveries and receive constant deals and recommendations. This creates a sense of comfort and choice. Platforms promise speed and low prices for customers, alongside flexible income for workers.

Zuboff provides a broader context for this story. She describes "surveillance capitalism" as a new stage of capitalism. **In this stage, companies treat human experience as raw material.** They record behaviour, extract "behavioural surplus", train prediction models, and sell "prediction products" on markets for future behaviour (Zuboff, 2019). Wearables, social media, AI tools and other digital platforms fit this logic very well. They "record" daily life in detail. The platform's owner receives a continuous stream of behavioural data. This data can be connected to other sources, such as shopping history, geolocation, and social media activity. Platforms earn money as users share more and more of their personal, private, and social lives. In this process, the platform does not just react to human attention; it also organises, directs, fragments, and connects it with advertising companies through data previously extracted, analysed and organised. The same logic applies to sports, health, and productivity apps. The user believes they "check" the app freely, when in fact the app's design and notification system push them to return, compare, and adjust—thereby adding more data about their physiological life.

Although the main problem addressed in this analysis is the breach of privacy and the unauthorised extraction of personal data, it is important, with the rise of digital platforms, to raise the question of digital precarity. Santos places this in the framework of platform capitalism from the perspective of the semi-periphery (Santos, 2025). He shows how platforms support a model of capitalism that values flexibility, precarity, and constant self-promotion among workers, while deliberately choosing countries with weak labour and business regulations. In this model, people must act like small firms, which raises another legal issue regarding the regulation of workers' rights and security.

The digital consent

When "I accept" does not mean a real choice.

In practice, many companies design privacy notices and consent forms in ways that confuse users. People do not have the time, energy or specific knowledge to read twenty pages of legal language. They often click "accept" because they need the service. So they exchange their personal data for the digital product or service. The formal right exists, but the interface design makes it weak. The law assumes a rational subject that reads, decides, and controls data flows. The actual user acts within an environment that companies design to distract, confuse, and pressure them into "blindly" accepting. If we seriously want to protect people, we must connect data protection law with the actual practice.

European Union Legal Framework

The European Union tries to limit the harms of this system through law. The main law is the General Data Protection Regulation (GDPR), which plays a central role. The GDPR establishes fundamental principles for the processing of personal data, including lawfulness, fairness, transparency, purpose limitation, and data minimisation. The GDPR grants citizens rights such as access to their data, correction, deletion, and the right to object. In theory, it provides strong protection. As users, people can ask companies what data they hold, why they use it, and with whom they share it.

The EU also adopted the Artificial Intelligence Act, which regulates AI systems through a risk-based model. The Act bans certain uses, such as social scoring by public authorities, while classifying others as high-risk—for example, AI systems in education, employment, health care, or critical infrastructure. Developers of high-risk systems must follow strict rules: collect high-quality training data, test the system, keep logs, and allow human oversight. Some AI applications in wearables or platforms fall inside these categories. Health-related risk predictions, affective computing, and automated content ranking are examples of AI tools that can significantly impact individual rights and freedoms.

The AI Act, therefore, matters for the business model that Zuboff describes. It does not ban surveillance capitalism, but it sets limits on some AI practices and demands greater transparency and safety. It aims to reduce the most serious harms while still accepting that companies build prediction systems for profit. As a result, the law improves some conditions but does not fundamentally alter the logic of extraction.

The Digital Services Act and the Digital Markets Act focus more directly on platforms. The Digital Services Act imposes duties on online platforms, especially the very large ones. They must assess systemic risks, including the spread of illegal content, threats to fundamental rights, harm to minors, and negative impacts on democratic processes. They must provide clearer information about recommendation systems and grant greater access to platform data for researchers. The Digital Markets Act targets gatekeeper firms and seeks to curb unfair practices that block competition, such as self-preferencing or forced bundling of services.

These acts recognise that platform companies now hold a special place in the economy and in public life. Lawmakers no longer see them as neutral intermediaries. They treat them as powerful actors that shape speech, trade, and attention. Still, the focus stays on transparency, accountability, and competition. The acts do not question the idea that platforms can base their profits on targeted advertising and continuous monitoring.

North Macedonia as a legal semi-periphery: copying the rules, but missing the power

North Macedonia occupies an interesting position in this context. The country is not an EU member but follows the path of EU integration. In 2020, it adopted a new Law on Personal Data Protection that aligns with the GDPR and incorporates similar concepts and principles. The law sets rules for data controllers and processors and grants rights to data subjects. The Personal Data Protection Agency serves as a supervisory authority.

Citizens of North Macedonia, therefore, live in a space where the law closely resembles EU law. Nevertheless, the country occupies a semi-peripheral position in global capitalism, as Santos describes. The main issue is that big technology firms do not base their headquarters there. Local regulators have less power than their counterparts in large EU member states, and many people use services from companies that respond more to authorities in Brussels, Dublin, or Washington than to institutions in Skopje. **This creates a gap between formal legal alignment and real power.**

And... what next?

All of this raises a simple but tricky question. What does the rule of law mean in a world of platforms, data extraction and AI tools? It cannot mean only that a country copies EU laws into its own legal system. It must also mean that real people can use those laws in practice and that public institutions have the strength to enforce them.

On the most intimate level, people need space for a private life. They need room to make mistakes, rest, and think without being tracked. When every step, message, and search query becomes data for someone else, privacy does not exist in a meaningful way. The rule of law should protect that space. It should limit how far platforms and devices enter into personal life. It should also recognise that people often act under pressure and confusion, not as perfectly informed, rational subjects.

On the economic level, surveillance capitalism and platform capitalism will not disappear simply because lawmakers adopt new laws. These models grow from deeper structures. Investors demand constant growth. Companies compete for attention and data. In this race, every new metric and every new prediction looks attractive. If we take the rule of law seriously, we have to ask how to put real limits on this race. That includes stronger competition rules, clear bans on the most harmful practices and serious sanctions for violations, not just symbolic fines.

On the institutional level, countries like North Macedonia need support, not only obligations. EU institutions, regional networks, and civil society can build alliances to give local regulators greater weight. Researchers and journalists can use new access rights under the DSA to study in greater detail how platforms operate. Education programs can help people understand their digital rights and recognise patterns and manipulative designs. The rule of law then becomes a living practice, not just a line in a progress report to Brussels.

For North Macedonia, the path to EU integration can open two different futures. In one, the country merely copies the rules while global platforms retain the real power, and people accept constant tracking as the price of modern life. In the other, lawmakers, regulators, experts, and citizens use the EU framework as a tool to push back. They treat data protection, AI regulation, and platform obligations as part of a wider struggle for justice and democracy.

Digital surveillance will not stop on its own. Platforms will not relinquish profitable data flows out of the kindness of their hearts. If the rule of law is to retain any meaning in this context, it must stand on the side of the people, not extraction. It must protect the right to stay untracked, the right to disconnect, and the right to exist without constant scoring. Only then can North Macedonia enter the EU as more than a legal copy—as a society that understands the digital future it wants and is willing to fight for it.