IOSR Journal Of Humanities and Social Science (IOSR-JHSS)
Volume 30, Issue 8, Series 5 (August, 2025) 24-33
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

The Interplay Between User Awareness And Transparency Requirements In The Context Of European Platform Regulation

Balázs Hohmann
(Department Of Technology Law And Energy Law, Faculty Of Law, University Of Pécs, Hungary)

Abstract:
Background*: Over the past two decades, online platforms in Europe have shifted from being relatively passive intermediaries to powerful actors that influence information flows, public opinion, and digital markets. Early voluntary initiatives failed to deliver consistent transparency or accountability, which led the EU to introduce binding frameworks — the Digital Services Act (DSA) and Digital Markets Act (DMA). Both build on the General Data Protection Regulation (GDPR) and national laws such as Germany's NetzDG, with the shared goal of tackling societal risks and limiting market dominance. Their effectiveness, however, depends not only on legal provisions but also on whether users can interpret and apply the information these rules require platforms to provide.*
Materials and Methods*: The study combines analysis of EU legislation, regulatory guidance, and academic literature. It traces the transition from self-regulation to binding legal regimes and examines how the DSA and DMA approach transparency, user rights, and systemic risk management. The assessment also considers overlaps with other legal instruments, national enforcement disparities, and the role of digital literacy in making transparency measures effective.*
Results*: The DSA and DMA introduce stronger safeguards — including clearer explanations of algorithmic processes, opt-out possibilities, and structured risk assessments. Yet practical barriers remain: national enforcement capacity varies, compliance costs weigh more heavily on smaller platforms, and technical disclosures often fail to reach or engage the average user. Without communication formats tailored to different literacy levels, transparency may end up as a formal requirement rather than a tool for user empowerment.*
Conclusion: *By replacing voluntary commitments with enforceable standards, the DSA and DMA mark a turning point in EU platform governance. Their long-term success will rely on ensuring that transparency is accessible and actionable, supported by consistent oversight and targeted education so that all users — not only the digitally skilled — can benefit from the protections these laws intend to provide.*
Funding: *This work was supported by the National Research, Development and Innovation Fund, provided by the Hungarian Ministry of Culture and Innovation, under Grant NKKP STARTING_24 (STARTING 150399) programme.*
Key Word*: Digital literacy; Platform regulation; Transparency; User Awareness.*
Date of Submission: 10-08-2025 Date of Acceptance: 20-08-2025

I. Introduction

Over the last decade, the online world has changed at a pace that few could have predicted. What began as a network of relatively simple services for communication and information sharing has grown into a dense, highly complex ecosystem (Bendiek, 2021; Madiega, 2022). Today's platforms do not just host content — they shape conversations, influence what information we see, and even affect how we think about public issues (Papp, 2025). This is not simply the result of better technology. It also comes from the fact that a small number of very large companies now control an outsized share of our digital environment (Jaursch, 2024). Such a rapid transformation has brought obvious benefits, but it has also raised serious concerns. The more central platforms become to our everyday lives, the more important questions arise about transparency, fairness, and accountability (Hacker et al., 2024; Çevik, 2023). In practice, these concerns are not limited to one country or one sector. They cut across social, political, and economic spheres, affecting individual users and society at large (de Andrade et al., 2023). Europe's earlier legal framework — particularly the E-Commerce Directive of 2000 — was built for a very different kind of internet. At the time, online platforms were smaller, more fragmented, and played a much less active role in filtering or amplifying information (MacCarthy, 2020). The last twenty years have made that framework look increasingly outdated. Today's digital giants operate with advanced data-driven models, complex algorithmic recommender systems, and large-scale content moderation

tools (Hacker et al., 2024). These tools do not merely respond to user activity; they shape it, often in ways that are invisible to the user (Papp, 2025).

The EU's adoption of the Digital Services Act (DSA) and the Digital Markets Act (DMA) is an attempt to catch up with this reality. These two laws are designed to work together: the DSA focuses on content governance, transparency, and the management of systemic risks, while the DMA aims to curb the market power of so-called "gatekeeper" platforms (Bendiek, 2021; Madiega, 2022). In other words, one targets the societal risks of platform behaviour, the other the economic imbalances that arise when a few companies dominate (Jaursch, 2024). These laws do not emerge in a vacuum. They are shaped by earlier European experience — most notably, the General Data Protection Regulation (GDPR) — and by national laws such as Germany's Network Enforcement Act (NetzDG) and France's Loi Avia (MacCarthy, 2020; Tourkochoriti, 2023). The GDPR significantly raised awareness of data protection and individual rights, but it also revealed practical problems: overly complex information, uneven enforcement between countries, and the challenge of making people actually understand the rules that protect them (Çevik, 2023; Madiega, 2022). The DSA and DMA try to address some of these weaknesses, for example by introducing stronger enforcement structures and recognising that smaller platforms cannot be held to exactly the same compliance demands as the largest players (Jaursch, 2024).

Transparency runs as a common thread through all of these measures. It sounds straightforward: platforms should explain what they do in ways people can understand. But in practice, this is harder than it looks (Anderson & von Seck, 2020). More information does not automatically mean better understanding. If disclosures are too long, too technical, or too scattered, people will not read them — or if they do, they may not make much sense of them (Hacker et al., 2024; Papp, 2025). Research on earlier regulations has shown this repeatedly (Çevik, 2023). That is why the DSA and DMA face the challenge of not just requiring openness but ensuring that openness works in reality, for different kinds of users with very different levels of digital literacy (Shin et al., 2022; de Andrade et al., 2023). Another crucial issue is enforcement. Passing a law is one thing; making it stick is another. The EU has assigned new responsibilities to national Digital Services Coordinators and given the European Commission a more active oversight role (Jaursch, 2024). But the history of the GDPR shows that enforcement can vary widely from one member state to another (Madiega, 2022). Without proper coordination, there is a risk that some platforms will face strict scrutiny while others will operate with far less oversight (Schwartmann et al., 2024). That would undermine the goal of equal protection for all users.

At the centre of this study is the relationship between transparency requirements and user awareness. The EU's platform laws aim not just to make platforms publish more information but to make that information genuinely usable — so that people can make informed choices, challenge unfair practices, and understand the systems that shape their online experience (Hacker et al., 2024; Papp, 2025). Achieving that balance is not easy. It will require clear disclosure formats, educational efforts, and enforcement that is both consistent and fair (Anderson & von Seck, 2020). The following chapters will explore how this balance might be struck, and what it will take for the EU's digital regulation to fulfil its promise of a safer, fairer, and more transparent online environment.

II. The Evolution Of European Platform Regulation

From Self-Regulation to a Binding Legal Framework

The European Union's journey from voluntary self-regulation to enforceable platform legislation was not a sudden leap, but rather the outcome of repeated disappointments with earlier approaches. In the 2000s and early 2010s, the prevailing idea was that platforms could be trusted to police themselves. Memoranda of Understanding (MoUs) promoted by the European Commission were a typical example. They called for greater transparency, more accountability, and stronger protection for users. In theory, these agreements suggested a shared sense of responsibility between regulators and digital companies. In practice, the results were underwhelming. The sale of counterfeit goods, for instance, continued despite formal commitments to stop it (Madiega, 2022).

The main problem was obvious: there was no real enforcement. Platforms could decide for themselves how, or even whether, to apply the measures they had promised. This discretion led to uneven implementation, with some companies taking visible steps while others did the bare minimum. Broader, systemic challenges—such as the spread of disinformation, hate speech, and other harmful content—remained largely untouched (Madiega, 2022).

There was also an imbalance of incentives. For the largest technology companies, commercial priorities usually outweighed any voluntary commitments to user protection. Firms like Facebook, Google, and YouTube, having secured dominant positions in their markets, could set unilateral terms of service and lock users into highly asymmetrical relationships (Papp, 2025). Market share data illustrate the problem clearly: Google has held close to 80% of the global search market, while Facebook and YouTube together account for around 70% of global social media activity (Bendiek, 2021). Such concentration made it even less likely that self-regulation

would lead to meaningful change. Meanwhile, public concerns over privacy, data exploitation, and the influence of platforms on democratic debate were growing louder. Revelations about the role of social media in spreading misinformation and harmful content added political urgency to the call for accountability (Bendiek, 2021). The introduction of the General Data Protection Regulation (GDPR) in 2018 marked a turning point. It moved away from voluntary commitments and imposed binding, enforceable duties — especially in data protection and transparency. The GDPR forced companies to meet high compliance standards and, in measurable terms, reduced some of the most intrusive data-collection practices (Madiega, 2022).

The regulation also gave users new tools, such as informed consent and data portability, which strengthened individual control over personal information (Madiega, 2022). However, these gains were tempered by the complexity of the rules. Many users found GDPR notices difficult to understand, and enforcement varied widely between EU member states (Papp, 2025). These gaps pointed to the need for a more harmonised and targeted set of rules—precisely what the Digital Services Act (DSA) and the Digital Markets Act (DMA) set out to provide. Both laws build on the GDPR's foundations but aim to close its blind spots. The DSA requires Very Large Online Platforms (VLOPs) to make their recommender systems more transparent and to offer users the option to opt out of personalised feeds (Bendiek, 2021). Whether these obligations can be presented in ways that users truly understand remains an open question (Papp, 2025). The DMA complements this by targeting "gatekeeper" platforms and introducing obligations on interoperability and data-sharing to counter anti-competitive behaviour (Bendiek, 2021).

The consequences of sticking with voluntary approaches had already become clear in the real world. Incidents of politically motivated violence, planned in part through social media channels, demonstrated the dangers of insufficient oversight (Bendiek, 2021). Even earlier EU initiatives, such as the Code of Conduct on countering hate speech online, proved too limited in scope to handle such risks effectively. These experiences made the case for flexible but enforceable legal frameworks — rules that could adapt to emerging threats while providing strong, consistent safeguards for users (Madiega, 2022).

The DSA and DMA therefore go further than symbolic commitments. They require systemic risk assessment, demand explanations for algorithmic decisions, and reinforce user rights (Bendiek, 2021). From the perspective of contract law, they also push back against the long-standing use of adhesion contracts—non-negotiable terms imposed on users—which have been a defining feature of the digital economy (Ungureanu, 2021). In moving away from opaque, one-sided agreements toward enforceable obligations, these acts attempt to rebalance the relationship between platforms and their users. In essence, the DSA and DMA are the legislative outcome of lessons learned from the shortcomings of self-regulation. By embedding clear, enforceable standards of transparency, fairness, and accountability, they aim to address the realities of today's platform-driven digital environment, something voluntary measures were never equipped to do (Madiega, 2022).

The Digital Services Act and Digital Markets Act

The Digital Services Act (DSA) stands out as one of the European Union's most far-reaching attempts to bring coherence to the fragmented rules of the online marketplace. It covers an enormous range — over 10,000 platforms, from social media networks and search engines to online marketplaces — so the idea is not just to rein in the dominant players but to set a basic level of responsibility for everyone (Jaursch, 2024). In essence, the goal is to shield users from harmful content and to push for a more transparent and fair digital space. The law's reach is deliberate: it sends a signal that the responsibility to protect users does not rest solely on the tech giants, even if they inevitably bear the heaviest obligations.

A particular focus, however, falls on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)—those with over 45 million monthly active users in the EU. Their size gives them a decisive role in shaping information flows and market dynamics, which is why they face the strictest oversight. The DSA asks them to take a hard look at systemic risks such as the spread of harmful material, disinformation, or manipulative design practices (Bendiek, 2021). But here lies a delicate balance: while major platforms are obvious targets, smaller and more niche services can still become spaces where harmful narratives spread unchecked. The challenge is to avoid focusing so narrowly on the big players that these smaller but potentially dangerous corners are overlooked. One of the more tangible innovations is the requirement for internal complaint-handling systems. Compared with earlier voluntary schemes, such as the EU's Code of Conduct on countering hate speech, this is a step up. Now, users have a formal channel to contest platform decisions, and platforms are obliged to respond according to defined rules. In principle, this should build trust. Yet, as Tourkochoriti (2023) notes, the real-world test will be whether these systems can handle high volumes of complaints quickly and without becoming buried in bureaucracy. For smaller companies, the procedural load could be a serious drain on resources.

The DSA also introduces strict timelines for tackling illegal content—most notably, the expectation that flagged material will be reviewed within 24 hours. This is an ambitious benchmark and a clear signal of the EU's intention to limit the reach of harmful material. But it is equally clear that for platforms without large

moderation teams or advanced automated systems, meeting such deadlines will be a struggle (Tourkochoriti, 2023). There is a real possibility that smaller operators will slip into non-compliance, not out of disregard for the rules but simply because they cannot match the speed of the largest firms.

Transparency, unsurprisingly, sits at the centre of the DSA's design. Platforms must now explain how their algorithmic recommender systems work and give users the option to opt out of personalised feeds ([Bagni & Seferi, 2025). This is a positive move in principle—greater user control, fewer hidden biases—but there is no guarantee that the average person will understand, let alone use, these options. Digital literacy levels remain uneven across the EU, and as Papp (2025) points out, simply providing the information does not mean it will be absorbed. For transparency to be more than a procedural tick-box, the information needs to be digestible and genuinely useful.

The Digital Markets Act (DMA) works alongside the DSA but targets a different structural issue: the power of "gatekeeper" platforms. These are companies with enormous market reach—over 45 million EU monthly users or a market value above €65 billion—that can, in effect, set the rules for entire markets (Bendiek, 2021). Unlike the DSA's reactive model for handling risks, the DMA takes a proactive stance, imposing obligations designed to prevent anti-competitive behaviour before it takes root (Polyák et al., 2021). That includes banning self-preferencing, requiring interoperability between services, and creating fairer access to data. Data asymmetry is one of the DMA's main concerns. When dominant platforms control massive data sets that competitors or users cannot match, the imbalance is obvious. The DMA's data-sharing provisions try to close this gap. But as Cabral et al. (2021) note, the solution is not without its own risks—especially around privacy and security, which become even trickier when data moves between services. Any safeguards must be strong enough to avoid abuse while still encouraging the openness the law is supposed to promote.

Like the DSA, the DMA also insists on transparency in cross-service data processing where user consent is absent. The aim is to give users a clearer picture of how their personal information travels, though actually mapping those flows in a way that makes sense to non-specialists is no easy task (Hacker et al., 2024). In very large ecosystems, even insiders struggle to track every movement of data, so translating this into user-friendly language will be a major challenge.

Seen together, the DSA and DMA represent a wider EU strategy: to tackle the concentration of market power, contain systemic risks, and protect the integrity of the digital public sphere. The DMA's focus on interoperability and fair competition — in advertising markets, mobile ecosystems, and beyond — recognises that market structures directly shape user experience. But this is a balancing act: rules that are too rigid could choke innovation or discourage investment (Cabral et al., 2021). Enforcement is perhaps the most uncertain part of the picture. Both acts rely on national Digital Services Coordinators (DSCs) to oversee compliance, but the reality is that resources and expertise vary significantly between member states (Jaursch, 2024). This echoes the uneven application of the GDPR, where some regulators struggled to monitor major cases effectively. Smaller platforms also face a familiar problem — meeting compliance demands can be disproportionately costly, leaving them at a competitive disadvantage (Madiega, 2022). If member states interpret or enforce the rules differently, the EU risks ending up with a fragmented approach. Stronger, central oversight by the European Commission could help, but that requires sustained political agreement (Jaursch, 2024). In the end, the DSA and DMA are not static texts. They will need to evolve with the digital environment, adapt to new risks, and fine-tune their mechanisms if they are to remain effective and fair over the long term (Söderlund et al., 2024).

III. User Awareness In Digital Platforms

In the modern online environment, it takes more than knowing how to use an app or click through a website to truly navigate platforms. Real engagement depends on understanding how transparency measures work, how algorithms make decisions, and what rights the law gives to users. Without that, even the most ambitious rules under the Digital Services Act (DSA) and Digital Markets Act (DMA) can miss their mark. The gap between what regulators intend and what users can actually do remains one of the most pressing issues. Strengthening user awareness—through education, accessible tools, and targeted literacy efforts—is not just helpful but essential if these frameworks are to deliver on their promise of a fairer and more accountable digital space.

Conceptual Framework and Digital Literacy

Digital literacy forms the base for any meaningful engagement with platform regulation. It gives people the ability to find, understand, and critically assess both the services they use and the transparency mechanisms meant to protect them. Provisions in the DSA — especially those explaining how algorithms and recommender systems operate — implicitly assume that users already have a basic grasp of these concepts. In reality, many do not. As Papp (2025) shows, users often lack the confidence or knowledge to use these tools critically. Without that literacy, transparency stops short of fostering informed choice and autonomy. This gap directly affects trust. People who do not understand how algorithms shape their news feeds or search results are less likely to use the

available controls, and less likely to believe those controls will work (Shin et al., 2022). That undermines the DSA's empowerment goals. Skills are unevenly spread across Europe: younger, more digitally fluent groups are generally more active in using rights under laws such as the General Data Protection Regulation (GDPR), while older or less experienced users are often left behind (Rughiniş et al., 2019).

The GDPR offers a warning. Legally sound consent forms have often been so complex that they confuse users, leading to disengagement rather than control (Çevik, 2023). The same risk exists for the DSA and DMA if algorithmic transparency is not paired with plain language and user-friendly design (Hacker et al., 2024). For that reason, targeted interventions matter. Education programmes should prioritise groups most at risk—older adults, people with limited formal education, or communities with low internet access. Scenario-based learning, such as showing step-by-step how to change privacy settings or interpret personalised recommendations, can make rights more tangible (Çevik, 2023). The design of the tools themselves is equally important: dashboards, infographics, and interactive tutorials generally work better than static legal text (Shin et al., 2022).

Awareness of algorithms goes beyond knowing they exist—it involves understanding why they produce certain results. This kind of literacy narrows the data gap between platforms and users, a key aim of the DMA (Hacker et al., 2024). In this way, digital literacy is not just an add-on to regulation but part of the machinery that makes it work. Collaboration is the most promising way forward. Regulators, educators, and platforms can work together to create standardised resources, launch targeted campaigns, and adapt materials to different languages and cultural contexts (Madiega, 2022). Done well, this ensures that the rights in the DSA and DMA are not just words on paper but tools people can actually use.

Platform Transparency Requirements

The DSA and DMA both target two core challenges: cutting through algorithmic transparency and making platforms more accountable. The DSA requires platforms to explain how their recommender systems work, including the logic behind content personalisation, and to give users the option to opt out. While these rules are designed to empower, they only work if people can understand the explanations (Papp, 2025; Hacker et al., 2024). Without better literacy, transparency risks becoming a box-ticking exercise. The GDPR's history reinforces this concern. Consent mechanisms, though groundbreaking for privacy, were often too complex for most users to navigate (Çevik, 2023; Madiega, 2022). There's a real chance that DSA opt-out tools could follow the same path if they're not supported by intuitive design and clear guidance.

Another DSA innovation is the requirement for Statements of Reasons (SoRs) — public explanations for content moderation actions. This is intended to improve accountability and trust. Yet early findings from the DSA Transparency Database show that 99.8% of SoRs relate to breaches of Terms of Service, and only 0.2% to clearly illegal content (Kaushal et al., 2024). This imbalance raises the question of whether the measure is really focused on the most serious harms. The DSA's emphasis on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) mirrors the DMA's focus on gatekeepers. However, smaller platforms can also spread harmful content, especially within niche communities. For them, compliance costs—already a burden under the GDPR—can be even harder to manage (Madiega, 2022; Jaursch, 2024). Proportionality is key: rules should be strong enough to protect users but scaled to fit the resources of different platforms.

In the DMA, transparency rules focus on data imbalances, requiring gatekeepers to explain any cross-service data processing done without explicit consent. The difficulty, again, is making these explanations meaningful to people with very different levels of technical knowledge (Hacker et al., 2024). Germany's Network Enforcement Act (NetzDG) provides a practical example. Its regular, standardised reports on content moderation have helped improve both accountability and public trust (MacCarthy, 2020; Jaursch, 2024). A similar approach at EU level could help avoid fragmentation in how the DSA and DMA are enforced.

Ultimately, transparency mechanisms only succeed if they close the gap between legal ambition and user capacity. Tools like layered disclosures, visual summaries, and interactive explanations—combined with targeted literacy initiatives—can turn transparency into a real form of empowerment (Anderson & von Seck, 2020; Hacker et al., 2024). When designed with users in mind, the DSA and DMA have a much greater chance of meeting their ultimate goal: a more open, fair, and accountable digital ecosystem (Shin et al., 2022; Madiega, 2022).

IV. Impact Of European Regulations

The adoption of the Digital Services Act and the Digital Markets Act represents a major shift in how the EU approaches platform governance. These two frameworks reach into almost every aspect of the online environment — from the rights users can exercise and the transparency platforms must offer, to how systemic risks are identified and how rules are enforced across borders. Their influence goes well beyond ticking legal compliance boxes: they are reshaping how platforms, regulators, and users interact in practice. This chapter looks at what these changes mean on the ground, focusing not only on the gains in user empowerment the

lawmakers intended, but also on the frictions that emerge when broad legislative ambition meets the messy realities of day-to-day implementation. Both the DSA and DMA set out to strengthen transparency, reinforce user rights, and hold dominant platforms to account. Whether they can deliver on that promise depends on three things: how their rules are interpreted, how they are enforced, and — perhaps most importantly — how well they are understood by the people they are meant to protect. While the legislative texts define obligations in detail, the way they play out in real-life user experiences is far less straightforward.

Transparency Obligations

Transparency is a central pillar of the DSA, especially for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) services with more than 45 million monthly active users and significant power over how information flows online. These services must identify and assess systemic risks, such as the spread of misinformation or the amplification of harmful content and then disclose their findings. In theory, these reports are a blueprint for accountability; in practice, they are often written in technical language that most users will never fully grasp (Hacker, 2024; Madiega, 2022).

Educational and digital literacy gaps across the EU make this even harder. For someone with limited technical knowledge, the average algorithmic transparency report is dense and impenetrable (Ződi, 2022). As Hacker (2024) and Jaursch (2024) point out, platforms rarely make the effort to repackage these risk assessments into formats that work for everyday audiences. Without creative communication tools — visual dashboards, interactive explanations, or plain-language summaries — the gap between formal compliance and actual understanding will likely remain (Ződi, 2019).

One of the most high-profile transparency measures in the DSA is the requirement for VLOPs to explain how their recommender systems work, alongside the option for users to opt out of personalised content. This should, in principle, help people think more critically about how platforms shape their online experience. Yet evidence suggests these disclosures fail to connect with most users (Papp, 2025; Çevik, 2023). The GDPR experience offers a cautionary tale: when consent forms are too long or too complex, users tend to disengage entirely. If algorithmic logic is presented in a way that feels abstract or overly technical, the measure risks becoming a procedural formality rather than a real tool for empowerment.

Opt-out functions face similar hurdles. Poorly designed interfaces or overly complicated steps can make users abandon the process altogether (Madiega, 2022; Çevik, 2023). Statements of Reasons (SoRs), intended to explain why a piece of content was moderated, also run into trouble. Kaushal et al. (2024) found that almost all SoRs (99.8%) relate to breaches of Terms of Service, while only a tiny fraction address illegal content. That imbalance, combined with the legalistic tone of many statements, raises doubts about whether the measure is targeting the most pressing issues or making sense to a general audience.

For smaller platforms, the challenge is different but equally significant: cost. Even if they are not VLOPs or gatekeepers, they may still host harmful content and thus fall under certain obligations. Producing detailed reports or compliance documentation can be disproportionately expensive — a pattern already seen under the GDPR (Madiega, 2022; Jaursch, 2024). Here, proportionality is key: scaling obligations according to platform size or offering technical support could help maintain diversity and competition online.

The DMA's transparency rules address a narrower but important issue — the data advantage that gatekeeper platforms hold. For example, they must now explain in plain terms why they are processing user data across different services without consent. The idea is to open up business practices that were once opaque. But as with the DSA, meaningful transparency is not guaranteed if the audience lacks the background to interpret these disclosures (Hacker et al., 2024; Jaursch, 2024). Germany's Network Enforcement Act (NetzDG) provides a helpful reference point: its structured and regular content moderation reports have shown that standardised formats can make public reporting more comprehensible and enforcement more consistent (MacCarthy, 2020; Jaursch, 2024).

In the end, transparency only works if it can be understood. Layered disclosures, plain-language summaries, and visual tools — combined with targeted digital literacy initiatives — can transform it from a compliance exercise into something that genuinely helps users make informed decisions (Anderson & von Seck, 2020; Hacker et al., 2024).

User Rights and Control

One of the more visible changes under the DSA is the obligation for platforms to put their rules and processes into language that people can actually follow. This means publishing terms of service that do not read like a legal textbook, explaining—in plain words—how their recommender systems work, and giving reasons when they take down content. The intention is clear: to help users make sense of what is happening on the services they use every day. Yet, as Madiega (2022) points out, the volume and tone of these documents often discourage readers before they reach anything important. The explanations of recommender systems show this

gap well. They are supposed to reduce the imbalance of information between platforms and users, but in many cases the technical language remains a barrier (Papp, 2025). The "Statements of Reasons" meant to justify moderation decisions suffer from a similar problem. According to Kaushal et al. (2024), almost all — 99.8 percent — refer to breaches of Terms of Service, while just 0.2 per cent address illegal content. That imbalance raises doubts about whether the tool is tackling the most serious risks. Opt-out buttons for personalised feeds are another example where the law's promise and everyday reality do not always meet. People with less digital experience may not be sure what opting out really changes, and badly designed menus can make the option hard to find or use (Hacker, 2024). Here, more intuitive visuals, short tutorials, and designs tested with real users could make the difference between a formal right and a practical choice.

The DMA adds to this picture by giving users stronger rights over their own data, including the ability to take it with them to other services. On paper, this should boost competition. In reality, it runs into messy technical details: data formats that do not match, processes that are not enforced consistently (de Streel & Robertson, 2024; Jaursch, 2024). Experience from the GDPR shows that step-by-step guidance and automated export tools can make portability far easier to use (Miller et al., 2024). Because the DSA, DMA, and GDPR overlap, users can end up wading through multiple notices, all asking for attention. While these laws work towards similar aims, the layering of different disclosure and consent rules risks producing fatigue rather than clarity (Madiega, 2022; de Andrade et al., 2023). Pulling the requirements together—through shared formats or coordinated notification styles—would help keep the original intent without exhausting the audience (Schwartmann et al., 2024). The AI Act adds one more dimension: users must be told when they are interacting with AI systems. Research suggests that a clear banner or prompt works much better than a page of legalese (de Andrade et al., 2023; Papp, 2025).

Finally, there is the matter of enforcement. National regulators vary in resources and approach, which means that the same rule can be applied unevenly across the EU. Smaller platforms, in particular, often lack the capacity to keep up (Schwartmann et al., 2024; Bendiek, 2021). Germany's NetzDG shows how a standardised reporting system can help. A stronger coordinating role for the European Commission—backed by financial and technical support—could go a long way towards levelling the field.

GDPR and AI Act Influence

The GDPR has been in place long enough to show both the value and the limits of transparency rules. Its focus on accountability and data protection overlaps closely with the DSA's goals—especially when it comes to explaining how algorithms work and identifying systemic risks for large platforms (Butt, 2024). Yet the same stumbling block keeps appearing: even when the information is available, many users simply do not understand it (Madiega, 2022; Papp, 2025). Another challenge is that the GDPR has never been enforced in quite the same way everywhere. Some countries have strong, well-resourced authorities; others do not. Those gaps in capacity and interpretation are likely to repeat themselves under the DSA unless there is stronger coordination from the European Commission and more consistent guidance across the EU (Schwartmann et al., 2024). The GDPR's principle of data minimisation could help here. By limiting the amount of personal data collected, platforms can also reduce the complexity of what needs to be explained. But finding the right balance is tricky: users need enough detail to hold platforms accountable, without being buried under pages of technical disclosures (Madiega, 2022; Butt, 2024).

The AI Act adds another layer of regulation, this time built around a risk-based system. AI providers must document how their systems work, what they can and cannot do, and what risks they pose. In theory, this complements the DSA's transparency aims. In practice, it means more forms, more reports, and more demands on both staff and budgets—especially for smaller platforms that have fewer resources (Hacker et al., 2024; Nizza, 2024). Standardised templates and joint reporting systems could prevent the duplication of effort and make it easier to meet all these overlapping rules.

Both the AI Act and the GDPR stress the importance of human oversight and ethical standards. But complying with two sets of demanding obligations—data protection and AI transparency—can be tough for even the bigger companies. For smaller ones, it risks reinforcing the market power of those already at the top (Schwartmann et al., 2024; Butt, 2024). Practical support, from toolkits to subsidies, could help balance the scales. One clear lesson from the AI Act is that design matters. When people are told they are interacting with AI, they tend to respond far better to a simple banner or pop-up than to a dense legal notice (de Andrade et al., 2023). That same principle applies across all these frameworks: the way information is presented can matter just as much as the content itself. Taken together, the GDPR, AI Act, DSA, and DMA are all pulling in the same direction—towards a more transparent and accountable digital environment. But without coordination, they risk creating a maze of overlapping rules. Shared tools, consistent enforcement, and user-centred design could help ensure these laws strengthen each other rather than overwhelm the very people they are meant to protect (Schwartmann et al., 2024; Bendiek, 2021).

V. Recommendations For Enhanced User Awareness

Digital regulation in the EU has grown far more ambitious in recent years. The DSA and DMA are not just sets of rules for platforms; they are attempts to reshape the relationship between users, companies, and regulators. But the success of these laws rests heavily on whether users understand what's going on behind the interface and feel empowered to act on that knowledge. This chapter outlines two connected strands of action: compliance strategies that make transparency practical, and engagement approaches that help users actually use the information they are given.

Platform Compliance Strategies

Transparency is a legal requirement under the DSA, but it is also a design choice. Platforms have to decide how they will present information about complex systems like recommender algorithms. Too often, disclosures are drafted for lawyers and engineers, not for everyday users (Papp, 2025). That means they get lost in dense language or technical diagrams. One practical step forward is to use plain language, visual summaries, or even interactive tools that show how data flows. Of course, oversimplifying has its own risks—important details can be lost, and the point of transparency is not to offer a half-truth. The challenge is to balance clarity with completeness, and to create formats that suit different levels of digital literacy. Different groups need different approaches. Research shows that factors like age, education, and technical confidence shape how people interpret and respond to personalised content (Hacker et al., 2024). A teenager who has grown up with TikTok might already understand the basics of algorithmic curation, while an older user might value a simple, clear opt-out button. Platforms that want to build trust should tailor their transparency measures accordingly—using different explanations, adapting language, and making sure opt-out options are easy to find and use. It's not cheap to do this at scale, but inclusivity rarely is.

Interactive tools are another promising route. Dashboards that let users see how their behaviour shapes recommendations can make abstract processes more tangible (Papp, 2025). They fit neatly with the DSA's vision of informed user control, but building them requires investment—both technical and financial—that small platforms may struggle to afford. Without support, these innovations risk being concentrated among big players, deepening inequality in compliance. This is one area where regulators could step in with targeted guidance or funding.

Compliance cannot be an afterthought. Platforms that integrate transparency into their broader corporate strategy—through dedicated legal and technical teams, regular algorithmic audits, and external assessments—tend to be better prepared for regulatory changes (Hacker et al., 2024; Bauer et al., 2022). Independent review boards, tasked with checking how transparency commitments are met, could strengthen this further (Madiega, 2022). But here too, there are trade-offs: these boards need resources, clear mandates, and cooperation from management to have real impact. Feedback loops matter. Under the DSA, platforms must have complaint-handling systems, but the best ones don't just resolve issues—they spot patterns, feed lessons back into design, and help prevent repeat problems (Tourkochoriti, 2023). Aligning these mechanisms with GDPR-style consent requirements can streamline the user experience (Hacker et al., 2024), though combining regulatory frameworks inevitably adds complexity. Centralised dashboards for managing both privacy and transparency settings could help, but they require cross-regulatory thinking and cooperation between policymakers and platforms (Butt, 2024).

Finally, there is scope for more creative governance. Contracts that clearly define how partners handle data, regular public updates, or even blockchain-based systems for tracking data use can reinforce accountability (Li, 2023; Hacker et al., 2024). And while collaboration with regulators and auditors can be time-consuming, it's also a way to anticipate shifts in the legal landscape and stay ahead of enforcement (Madiega, 2022). For smaller platforms, though, this all comes down to resources—without enough people or funding, even the most willing company will struggle to keep up.

User Engagement Guidelines

Compliance strategies only work if users actually engage with them. That means presenting information in a way that is accessible, relevant, and worth the user's time. Under the DSA, platforms are expected to explain policies on moderation, data use, and algorithms. But too often, those explanations are heavy with technical or legal language (Anderson & von Seck, 2020; Papp, 2025). The result? Many users skip them entirely. There are obvious fixes. FAQs, video explainers, and visual guides can help break down barriers, especially for those with lower digital literacy (Rughiniş et al., 2019; Hacker et al., 2024). The key is to balance simplicity with accuracy—simplifying too far risks misleading people. Ethical design plays a role here too. Removing manipulative "dark patterns" from consent processes builds trust and aligns with DSA principles (Çevik, 2023). Platforms should be proactive in auditing themselves for such practices before regulators force their hand.

Interactive tools can go beyond mere compliance. Dashboards that show why a post or video is being recommended, or tutorials that walk users through content moderation rules, turn abstract rights into something

tangible (Anderson & von Seck, 2020; Papp, 2025). But these features are costly to build and maintain, which again raises the issue of supporting smaller platforms. User participation can improve both trust and design quality. Surveys, focus groups, and community consultations can give platforms direct insight into what people actually need (Jaursch, 2024). To work, these processes have to be inclusive—covering not just the tech-savvy majority, but also users with disabilities or limited online experience (Söderlund et al., 2024; Çevik, 2023). Publicly reporting on the feedback received, and on what changes were made as a result, can close the loop and make the process more than a box-ticking exercise (Papp, 2025). Communication should be tailored. Those with limited digital skills might prefer step-by-step visual instructions, while more advanced users could value deeper insight into algorithmic logic (Hacker et al., 2024; Anderson & von Seck, 2020). User testing before rolling out new features can reveal which approaches actually work (Jaursch, 2024), though it adds time and cost.

Education has to be part of the picture. Workshops, webinars, and partnerships with schools or universities can raise baseline digital literacy (Rughiniş et al., 2019; Goddard, 2017). Online self-paced courses, developed with regulators, could reach even wider audiences (Shin et al., 2022; Hacker et al., 2024). Here again, inclusivity is key — training that overlooks vulnerable groups will only widen existing gaps.

Ultimately, engagement is about trust. Platforms that are transparent about what data they collect, why they collect it, and what they don't collect are better placed to win user confidence (Madiega, 2022; Hacker et al., 2024). Independent audits under the DSA, DMA, and GDPR could reinforce this trust, provided they are well-funded and credibly run (Jaursch, 2024; Madiega, 2022). Bringing these strands together, user engagement under the DSA is not just about meeting legal obligations. It's about designing systems that people can—and want to—interact with, while being honest about trade-offs and limits. The closer those systems align with users' actual needs, the stronger the impact of transparency will be.

VI. Conclusion

This research examined how the EU's shift from self-regulatory approaches to binding legislative frameworks — most notably the DSA and DMA — has influenced user awareness and the implementation of transparency obligations in digital governance. It analysed the interaction between regulatory structures and user comprehension, asking whether these legal instruments enhance accountability, build trust, and enable users to navigate an increasingly complex online environment. By tracing the development of platform regulation, assessing how transparency measures operate in practice, and evaluating their alignment with the GDPR and AI Act, the study offered a detailed account of how these instruments seek to address long-standing shortcomings in platform governance. Drawing on academic literature, regulatory evaluations, and practical examples, it critically assessed the role of user awareness in advancing transparency and accountability.

The findings show that the weaknesses of earlier self-regulatory models — most notably discretionary enforcement and the dominance of platform-led solutions — prompted the move towards binding legal obligations. The GDPR provided an essential foundation but revealed challenges in ensuring consistent enforcement and meaningful user engagement. Building on this, the DSA addresses systemic risks linked to VLOPs and VLOSEs, such as algorithmic bias, misinformation, and harmful content amplification. The DMA complements this by tackling anti-competitive behaviour among gatekeepers through interoperability requirements, data-sharing mandates, and safeguards for fair competition. Together, these frameworks signal a decisive evolution in EU digital governance, yet their effectiveness ultimately depends on users' ability to understand and engage with transparency measures.

A central finding is that digital literacy remains a major barrier to the success of transparency measures. While the DSA and DMA require disclosures of algorithmic processes, opt-outs from personalised recommendations, and detailed transparency reports, these often remain inaccessible to large segments of the population. Overly technical or abstract disclosures can overwhelm users, undermining the empowerment goals at the heart of the DSA and GDPR. Current digital literacy initiatives are patchy and insufficiently targeted, leaving vulnerable groups—such as older users and those with minimal online experience — at a disadvantage.

The study also examined how existing frameworks shape the implementation of the DSA and DMA. The GDPR's consent and data protection principles have clear synergies with transparency obligations, but enforcement has been uneven, and users experience fatigue from repetitive consent requests. The AI Act's emphasis on algorithmic accountability supports the DSA's aims but adds layers of compliance complexity. Overlaps—particularly in disclosure and risk assessment requirements—can cause operational inefficiencies, disproportionately affecting smaller platforms with limited resources. Greater regulatory coherence and simplification would help avoid these pitfalls.

Enforcement remains a critical challenge. The decentralised model of appointing DSCs has resulted in varying oversight capacities across member states, risking a patchwork of enforcement that allows platforms to exploit weaker jurisdictions. Greater cross-border coordination, supported by more centralised oversight from the European Commission, could help ensure consistency and prevent regulatory arbitrage. Smaller platforms face particular difficulties. Even without the strictest obligations of the DSA or DMA, they carry significant

compliance responsibilities. High costs and limited technical resources risk putting them at a competitive disadvantage, potentially stifling innovation and reducing market diversity. Tailored support measures could help address this imbalance.

The research acknowledges its limitations. Given the early stage of DSA and DMA enforcement, empirical evidence is still scarce. The analysis relied mainly on secondary sources and legal-text reviews, which cannot fully capture the evolving dynamics of platform–user interaction. The focus on larger platforms also means that some smaller-platform challenges remain underexplored.

This work contributes to the wider discourse on EU digital governance by highlighting the interplay between transparency, user awareness, and enforcement. It situates the DSA and DMA within the longer trajectory of EU regulation, building on lessons from the GDPR and anticipating the implications of the AI Act. The ultimate test of these frameworks will be whether they can translate complex regulatory ambitions into practical, understandable, and empowering tools for users. Future research should examine how transparency measures function in practice across different demographic groups, evaluate the role of DSCs in harmonising enforcement, and explore scalable, inclusive digital literacy strategies. It should also consider the relationship between compliance costs and innovation, particularly for smaller entities, to ensure regulation supports rather than hinders competition and diversity.

Overall, the evolution of EU platform regulation marks a significant turning point in digital governance. The DSA and DMA provide a strong basis for addressing systemic risks and promoting fair competition, but their long-term success depends on informed and engaged users, as well as consistent and effective enforcement. Aligning legislative ambition with the realities of user engagement, platform diversity, and enforcement capacity will be essential to ensuring equitable and effective digital governance.

References

[1]. Anderson, D., & Von Seck, R. (2020). The GDPR And Its Impact On The Web. Technical University Of Munich. Https://Doi.Org/10.2313/NET-2020-11-1_01

[2]. Andrade, N. N. De, Galindo, L., Zarra, A., Heal, J., & Rom, S. (2023). Artificial Intelligence Act: A Policy Prototyping Experiment – Towards Informed AI Interactions: Assessing The Impact Of Notification Styles On User Awareness And Trust (Pp. 1–28). Open Loop.

[3]. Bagni, F., & Seferi, F. (Eds.). (2025). Regulatory Sandboxes For AI And Cybersecurity: Questions And Answers For Stakeholders. CINI's Cybersecurity National Lab.

[4]. Bauer, M., Erixon, F., Guinea, O., Van Der Marel, E., & Sharma, V. (2022). The EU Digital Markets Act: Assessing The Quality Of Regulation (No. 02/2022). ECIPE.

[5]. Bendiek, A. (2021). The Impact Of The Digital Service Act (DSA) And Digital Markets Act (DMA) On European Integration Policy (WP Nr. 02). Stiftung Wissenschaft Und Politik, Deutsches Institut Für Internationale Politik Und Sicherheit.

[6]. Butt, J. S. (2024). The General Data Protection Regulation Of 2016 (GDPR) Meets Its Sibling The Artificial Intelligence Act Of 2024: A Power Couple, Or A Clash Of Titans? JURIDICA, 20(2), 7–52.

[7]. Cabral, L. M. B., Haucap, J., Parker, G., Petropoulos, G., Valletti, T. M., & Van Alstyne, M. W. (2021). The EU Digital Markets Act: A Report From A Panel Of Economic Experts. Publications Office Of The European Union. Https://Doi.Org/10.2760/139337

[8]. Çevik, İ. (2023). Avrupa Birliği Dijital Hizmetler Yasası'nın Değerlendirmesi [Evaluation Of The European Union Digital Services Act]. YBHD, 8(2), 387–419. Https://Doi.Org/10.33432/Ybuhukuk.1273986

[9]. Hacker, P., Cordes, J., & Rochon, J. (2024). Regulating Gatekeeper Artificial Intelligence And Data: Transparency, Access And Fairness Under The Digital Markets Act, The General Data Protection Regulation And Beyond. European Journal Of Risk Regulation, 15, 49–86. Https://Doi.Org/10.1017/Err.2023.81

[10]. Jaursch, J. (2024). The Digital Services Act Is In Effect – Now What?. Stiftung Neue Verantwortung. Stiftung Neue Verantwortung.

[11]. Kaushal, R., Van De Kerkhof, J., Goanta, C., Spanakis, G., & Iamnitchi, A. (2024). Automated Transparency: A Legal And Empirical Analysis Of The Digital Services Act Transparency Database. In ACM Conference On Fairness, Accountability, And Transparency (ACM Facct '24), June 3–6, 2024, Rio De Janeiro, Brazil (Pp. 1–19). ACM. Https://Doi.Org/10.1145/3630106.3658960

[12]. Maccarthy, M. (2020, February 12). Transparency Requirements For Digital Social Media Platforms: Recommendations For Policy Makers And Industry (Working Paper No. 3, Transatlantic Working Group On Content Moderation Online And Freedom Of Expression). Institute For Information Law, University Of Amsterdam. Https://Www.Ivir.Nl/Publicaties/Download/Transparency_Maccarthy_Feb_2020.Pdf

[13]. Madiega, T. (2022). Digital Services Act. European Parliamentary Research Service.

[14]. Papp, J. T. (2025). Moving Forward: Charting The Much-Needed Evolution Of The Digital Services Act. In M. Szabó, L. Gyeney, & P. L. Láncos (Eds.), Hungarian Yearbook Of International Law And European Law 2024 (Pp. 457–476). Nomos. Https://Doi.Org/10.5771/9783748946526-457

[15]. Polyák, G., Pataki, G., Gosztonyi, G., & Szalay, K. (2021). Versenyjogi Előzmények És Piacszabályozási Eszközök A Digitális Piacokról Szóló Európai Rendelet Tervezetében [Competition History And Market Regulation Tools In The Draft European Regulation On Digital Markets]. In P. Valentiny, K. Antal-Pomázi, Z. Berezvai, & I. Nagy Csongor (Eds.), Verseny És Szabályozás 2021 [Competition And Regulation 2021] (Pp. 145–161). Centre For Economic And Regional Studies.

[16]. Rughiniş, R., Rughiniş, C., Vulpe, S. N., & Rosner, D. (2019). From Social Netizens To Data Citizens: Variations Of GDPR Awareness In 28 European Countries. University POLITEHNICA Of Bucharest.

[17]. Shin, D., Kee, K. F., & Shin, E. Y. (2022). Algorithm Awareness: Why User Awareness Is Critical For Personal Privacy In The Adoption Of Algorithmic Platforms? International Journal Of Information Management, 65, 102494. Https://Doi.Org/10.1016/J.Ijinfomgt.2022.102494

[18]. Söderlund, K., Engström, E., Haresamudram, K., Larsson, S., & Strimling, P. (2024). Regulating High-Reach AI: On Transparency Directions In The Digital Services Act. Internet Policy Review, 13(1), 1-31. Https://Doi.Org/10.14763/2024.1.1746

[19]. Tourkochoriti, I. (2023). The Digital Services Act And The EU As The Global Regulator Of The Internet. Chicago Journal Of International Law, 24(1), 129–147.
[20]. Ungureanu, C. T. (2021). Cyberspace, The Final Frontier? Concluding And Performing Agreements. Unfair Terms In B2B Adhesion Contracts. Analele Ştiinţifice Ale Universităţii „Alexandru Ioan Cuza" Din Iaşi, Tomul LXVII, Supliment 2, 9-24. Https://Doi.Org/10.47743/Jss-2021-67-4-1
[21]. Ződi, Z. (2022). Algorithmic Explainability And Legal Reasoning. Theory And Practice Of Legislation, 10(1), 67–92. Https://Doi.Org/10.1080/20508840.2022.2033945
[22]. Ződi, Z. (2019). The Limits Of Plain Legal Language: Understanding The Comprehensible Style In Law. International Journal Of Law In Context, 15(3), 246–262. Https://Doi.Org/10.1017/S1744552319000260