Computer Law & Security Review 59 (2025) 106181

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

# The regulation of social media commerce under the DSA: A consumer protection perspective

Laura Aade

*Faculty of Law, Economics and Finance, University of Luxembourg, 4 rue Alphonse Weicker, L-2721 Luxembourg, Luxembourg*

ARTICLE INFO

*Keywords:*
Social media commerce
Social media
Consumer protection
Digital Services Act
Platform liability
E-commerce

ABSTRACT

Social media commerce, defined as the direct selling of goods and services through social media, is emerging as a prominent business model in the platform economy. As social media platforms introduce e-commerce features, they are becoming what I call *social marketplaces:* a new category of online platforms found at the intersection of social networks and online marketplaces. This article examines how the Digital Services Act (DSA) protects consumers in relation to social media commerce, and what specific obligations it imposes on social marketplaces to increase transparency in online transactions. While the DSA does not explicitly address social media commerce, it indirectly applies through Section 4 which imposes obligations on 'online platforms allowing consumers to conclude distance contracts with traders'. I argue that because social marketplaces fall within this category of online platforms, they are subject to the obligations laid down in Section 4 DSA, namely Article 30 DSA (traceability of traders), Article 31 DSA (compliance by design), and Article 32 DSA (right to information). This article critically analyses the application of these provisions to social marketplaces and examines their interaction with EU consumer laws. Based on the analysis, it identifies three shortcomings in the DSA's approach to protecting consumers on social marketplaces: (i) regulatory complexity due to overlaps with the EU consumer *acquis*, (ii) interpretative ambiguity, as the DSA was not designed with social marketplaces in mind, and (iii) an enforcement gap specific to social media commerce. Rather than calling for new legislation, this article concludes that effective consumer protection on social marketplaces requires clarifying the interaction between legal instruments, interpreting existing provisions in light of evolving platform practices, and ensuring coordinated enforcement across relevant actors.

## 1. Introduction

The nature of social media has drastically changed over time. Initially, social media served as a space for users to connect and engage with each other by sharing content. However, the rise of new consumerist business models is creating a paradigm shift in the way social media are used today. Recognising the profitability of convenient online shopping experiences, several social media platforms have integrated e-commerce features into their services. Facebook launched its own 'Marketplace' for peer-to-peer transactions [1], TikTok introduced 'Video Shopping Ads' to boost product sales based on personalised advertising [2], and Instagram developed 'Shopping Tags' to reveal product features, price, and a link to purchase [3]. Social media are no longer just about social interactions, they are also becoming commercial hubs. This phenomenon is called social media commerce, and has transformed social media platforms into, what I call, social marketplaces.

This recent development raises questions about the protection of consumers who engage in commercial transactions with third-party sellers on social media. However, despite its growing relevance, social media commerce remains understudied from a consumer law perspective. Essentially, it is unclear which consumer protection rules apply to social media platforms adopting this emerging business model. In its report on the Digital Fairness Fitness Check, the European Commission classified social media commerce as a problematic practice for current consumer protection frameworks, which may not be sufficient to address this phenomenon [4]. Consequently, it is crucial to provide academic support to regulators and enforcement authorities in order to ensure that consumers are protected on social marketplaces, expected to be a game-changer for the digital economy [5].

This article analyses how the Digital Services Act (DSA) protects consumers in relation to social media commerce, and what specific obligations it imposes on social marketplaces to increase transparency in online transactions [6]. In doing so, it makes three innovative

*E-mail address:* laura.aade@uni.lu.

https://doi.org/10.1016/j.clsr.2025.106181

Available online 5 September 2025

contributions to existing scholarship found at the intersection of consumer protection and platform governance: (i) it sheds light on the e-commerce practices of social media platforms in the EU, (ii) analyses the impact of the DSA on consumer protection in the context of social media commerce, and (iii) assesses its coherence with legal instruments in the EU consumer *acquis,* highlighting both synergies and potential areas of tension. This article is structured as follows. First, it defines the concept of social media commerce and provides an overview of how social media platforms facilitate commercial transactions in the EU, distinguishing between formal and informal social marketplaces (Section 2). It then critically examines how the DSA applies to these emerging practices in order to protect consumers, focusing on the interplay with existing consumer laws (Section 3). In Section 4, I identify three shortcomings in the DSA's approach to consumer protection in social media commerce, before concluding (Section 5).

## 2. Social media commerce as a native way to shop on social media

### 2.1. What is social media commerce?

The concept of social media commerce is constantly evolving, resulting in a variety of definitions across disciplines [7]. A closer look at existing literature reveals two central approaches to defining social media commerce. It should be mentioned that this article uses the terms 'social media commerce' and 'social commerce' interchangeably, in line with the terminology adopted by the European Commission and existing literature.

The first approach to defining social media commerce focuses on its *social* aspect. Scholars highlight the influence of digital communities on shopping experiences through, for instance, the use of online reviews [8]. Kim defines social commerce as a *"subset of electronic commerce that uses social media, online media that supports social interaction and user contributions, to enhance the online purchase experience"* [9]. Similarly, Curty and Zhang emphasise the collaborative nature of social commerce, where users can interact in online spaces to explore shopping opportunities [10]. In that sense, social media platforms act as forums for peer-to-peer influence and validation: they shape purchasing decisions and consumer preferences through the power of online word-of-mouth [11]. This socio-centric perspective to social commerce reflects the proliferation of user-generated content on social media [12]. For instance, unboxing videos on YouTube allow content creators to document product experiences and influence viewers' purchasing decisions. More recently, live-streaming events hosted by brands on Instagram have become interactive spaces where audiences ask questions and discuss products features in real-time.

The second approach to defining social media commerce centers on its *transactional* aspect. It essentially focuses on the integration of e-commerce activities within social media ecosystems. According to Sturiale and Scuderi, social commerce is a *"special kind of e-commerce that allows the interaction between merchants and consumers in a social environment, such as Facebook"* [13]. Liang and Turban offer a similar definition, describing social commerce as *"the delivery of e-commerce activities and transactions via the social media environment"* [14]. Legal scholars, such as Goanta or Riefa, adopt this perspective by linking social commerce to the use of social media platforms in facilitating transactions [15]. In the same way, the European Commission describes social media commerce as the direct selling of goods and services to consumers through social media platforms [4]. And for that reason, I follow this transactional approach to social media commerce in this article.

### 2.2. How do social media platforms engage in e-commerce in the EU?

Defining social media commerce through a transactional lens mirrors the introduction of e-commerce features by social media platforms. This trend began around 2015 in the EU, when Facebook experimented with 'Buy Buttons' to facilitate direct purchases from brand pages [16]. Despite its innovative approach, the feature did not gain significant traction due to technical limitations as well as user hesitation [17]. However, the COVID-19 pandemic has sparked a renewed interest in social commerce, as the closure of physical stores and social distancing accelerated the shift towards online shopping. In response, an increasing number of social media platforms have (re-)integrated e-commerce features into their services [18], leading to the emergence of what I call *social marketplaces* – a new category of online platforms found at the intersection of social networks and online marketplaces (see Section 3.1 below).

Interestingly, the roll-out and sophistication of e-commerce features on social media vary not only between platforms, but also across EU Member States for the same platform. In some jurisdictions, social media platforms facilitate the entire shopping experience of consumers by allowing product discovery, by hosting product listings of third-party sellers, and by directly processing payments. In other markets, however, the same platforms may only provide partial e-commerce features: consumers interact with promotional content, but are redirected to third-party websites via in-app browsers to finalise their purchases. To reflect these variations, I distinguish between two types of social marketplaces, namely *formal* and *informal social marketplaces*, respectively described in the following sub-sections. This distinction is not merely descriptive and bears important legal implications: the extent to which a social media platform is involved in the transaction directly impacts how the DSA applies in practice and its level of compliance with the relevant provisions, as it will be shown in the analysis.

#### 2.2.1. Formal social marketplaces

Formal social marketplaces are social media platforms where the entire transaction journey, from product discovery to payment processing, is facilitated by the platform itself. They mirror the convenience and transaction flow of traditional e-commerce sites, such as Amazon or eBay [19], with one main difference: shopping is integrated into an interactive and social environment. Product discovery in this context is both intentional (e.g. via search tools) and ambient, emerging organically through everyday scrolling behavior, influencer promotion as well as algorithmic curation. What sets this category of social marketplace apart is the involvement of the platform which hosts product listings, enables in-app purchases, and processes payments directly.

A leading example is TikTok Shop, described by the platform itself as *"a completely personalised and fully integrated commercial solution, where sellers can authentically connect with creators and communities to drive meaningful shopping experiences"* [20]. After launching in the United States, Southeast Asia, and the United Kingdom, TikTok Shop entered the EU market in December 2024, starting with Ireland and Spain, after a series of delays [21]. As of this writing, TikTok Shop provides four native ways to shop on its infrastructure: (i) LIVE Shopping where users can buy products in real time during livestreams hosted by brands or creators, (ii) Shoppable Videos which embed clickable product links into short-form videos appearing in user feeds, (iii) Shop Pages which serve as curated storefronts linked to brand or creator profiles, and (iv) Shop Tab that is the dedicated marketplace interface of TikTok where consumers can browse products across categories, independently of their content feed. However, as the following sub-section will demonstrate, this level of e-commerce integration on social media is not yet uniform across the EU.

#### 2.2.2. Informal social marketplaces

In most EU Member States, social media platforms operate as informal social marketplaces. While they have incorporated elements of e-commerce (e.g. 'Show Now' buttons, product tags, or clickable links), these platforms do not directly support in-app purchases. Instead, when users engage with these elements, they are redirected to the third-party seller's website via the in-app browser of the app, bypassing the need for

external browsers like Safari or Chrome. According to Meta, this technique aims to enhance user experience by allowing them to view and interact with external web content without leaving the social media app [22]. It essentially removes the need to switch between apps or to re-enter information, such as credentials or URLs, to engage with content.

Consequently, the final steps of the transaction, such as entering payment details and completing the purchase, take place on the third-party seller's website – although consumers technically stay within the social media app [4]. Another defining feature of informal social marketplaces is that product discovery is largely passive and incidental. Consumers come across products while browsing organic content, but are not offered the tools to actively search, filter, or compare products within the platform itself. Table 1 below summarises the core differences between formal and informal social marketplaces, as introduced in both sub-sections.

## 3. Consumer protection rules relevant to social media commerce under the DSA

### 3.1. Social media commerce under the DSA

The DSA aims to safeguard and improve the functioning of the internal market for intermediary services by establishing rules for a safe, predictable, and trusted online environment [23]. While it addresses digital advertising [24] and consumer sales through online marketplaces [25], the DSA does not explicitly regulate issues related to social media commerce, such as in-app browsers or buy buttons [26]. However, I argue that it tackles it indirectly by providing a set of rules specifically applicable to 'online platforms allowing consumers to conclude distance contracts with traders' in Section 4 [27]. Whether social marketplaces fall within this category of online platforms is not expressly stated, but I take the view that they do for the reasons developed below.

'Online platforms allowing consumers to conclude distance contracts with traders' are typically referred to as 'online marketplaces' under European consumer law. Articles 2(17) of the Consumer Rights Directive (CRD) [28] and 2(n) of the Unfair Commercial Practices Directive (UCPD) [29] define an online marketplace as a *"service using a software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders and consumers"*. According to Recital 25 of the Modernisation Directive, this definition should be adapted to technology advancements in order to ensure its applicability to emerging technologies [30]. The European Commission, in its guidance on the application of the UCPD, further describes an online marketplace as an online platform enabling consumers to buy products offered by third-party suppliers *directly on its interface* (emphasis added) [31]. This interpretation suggests that, to legally qualify as an online marketplace, a social media platform must enable the transaction to be completed within its own interface, without requiring consumers to navigate away from its environment.

**Table 1**
Key differences between formal and informal social marketplaces.

| Feature | Formal social marketplaces | Informal social marketplaces |
|---|---|---|
| **Platform role in transaction** | Facilitates the entire transaction journey from product discovery to payment | Facilitates only part of the transaction journey, which is limited to product discovery |
| **Checkout experience** | Payment is processed directly by and on the platform | Payment is processed on external websites accessed through the platform's in-app browser |
| **Product discovery** | Both ambient (algorithmic feeds, influencer promotion) and intentional (via search tools) | Exclusively ambient, no tools available for structured search or comparison |
| **Availability in the EU** | Limited rollout, only available in selected EU Member States | Most common form of social media commerce in the EU, widely adopted across Member States |
| **Examples** | TikTok Shop (currently available in Ireland, Spain, France, Germany, and Italy), Instagram Shops with in-app checkout | Instagram posts with product tags, TikTok videos with 'Shop Now' buttons |

For formal social marketplaces (see Section 2.2.1 above), one can easily conclude that they meet the legal definition of an online marketplace. In such cases, consumers solely interact with the interface of the social media platform to purchase goods or products offered by third-party sellers. However, the same clarity does not apply to informal social marketplaces, where consumers are redirected to external websites via the in-app browser of the platform to complete transactions (see Section 2.2.2 above). This situation raises the following question: can the in-app browser of a social media app be considered part of its online interface (and by extension, can informal social marketplaces be legally classified as online marketplaces)? The answer depends on how the concept of 'online interface' is defined under EU law. Articles 2(16) of the Geo-Blocking Regulation [32] and 3(15) of the Consumer Protection Regulation [33] define an online interface as *"any software, including a website or an application, that is operated by or on behalf of a trader, and which serves to give consumers access to the trader's goods or services"* [34]. Given its embedded functionality, one could consider the in-app browser to be an integral part of a social media interface. Despite displaying content from third-party websites, it operates entirely within the technical and operational environment of the social media app. Its purpose is not merely to relay content, but to offer a seamless browsing experience – one that keeps consumers within the platform ecosystem, while facilitating access to external goods and services. What is crucial, however, is that in-app browsers are not passive or neutral conduits. As further discussed (see Section 3.2.3 below), social media platforms retain substantial control over these environments: they can monitor user behavior, track interactions, and even collect behavioral data when users navigate third-party content [35]. This level of oversight reinforces the view that in-app browsers are embedded interfaces operated by the platform itself. Accordingly, they satisfy both criteria to be legally considered part of a platform interface: in-app browsers are software operated by a social media provider that enable access to third-party goods or services.

Following this reasoning, both formal and informal social marketplaces qualify as online marketplaces, and hence as 'online platforms allowing consumers to conclude distance contracts with traders' under the DSA. However, the latter presents in its recitals 'social networks' and 'online platforms allowing consumers to conclude distance contracts with traders' as two distinct categories of online platforms [36]. Recital 13 DSA, for instance, explicitly refers to "online platforms, such as social networks *or* (emphasis added) online platforms allowing consumers to conclude distance contracts with traders" [37]. Although recitals have no binding legal force [38], this language nevertheless reveals that the DSA was drafted with these categories in mind as mutually exclusive – failing to recognise that social media platforms with e-commerce features also qualify as online marketplaces. As noted in the study supporting the Digital Fairness Fitness Check, the boundaries between social media platforms and online marketplaces are becoming increasingly blurred with the rise of social commerce [26]. In light of these developments, I argue that a new category of online platforms has emerged which lie at the intersection of social networks and online marketplaces: *social marketplaces*. Because such platforms legally qualify as 'online platforms allowing consumers to conclude distance contracts with traders', they must comply with the provisions set out in Section 4 DSA to protect consumers.

Before turning to a detailed examination of each provision in the context of social media commerce, the following section situates Section 4 DSA within the broader framework of EU consumer law. It first highlights how Section 4 DSA contains obligations directly relevant to

consumer protection and examines their intersection with the EU consumer *acquis*. Such analysis aims to shed light on the fragmented nature of the consumer protection regime applicable to social media commerce, as noted by the European Commission [4]. Building on this, it critically analyses how each provision of Section 4 DSA applies to social marketplaces and interacts with existing consumer protection instruments, such as the CRD and UCPD.

### 3.2. Section 4 DSA and the interplay with EU consumer law

Section 4 DSA contains three key provisions: Article 30 DSA on the traceability of traders, Article 31 DSA on compliance by design, and Article 32 DSA on the right to information. These provisions are directly relevant to consumer protection, as they aim to protect one specific category of recipients of the service, namely consumers. This focus is no coincidence. While the DSA is often associated with content moderation matters [39], it is equally committed to achieving a high level of consumer protection and effectively protecting fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, such as the principle of consumer protection [40]. This commitment to consumer protection is rooted in Article 12 of the Treaty on the Functioning of the European Union (TFEU), which requires the EU to take consumer protection into account while defining and implementing its policies as well as activities [41]. Interestingly, the consumer protection obligations found in the DSA illustrate a broader shift in the way EU consumer law is evolving today. Rather than relying on traditional contract law instruments like the CRD, consumer protection rules are increasingly emerging from public law market regulation, such as the DSA [42]. This shift aligns with what Micklitz refers to as 'regulatory EU private law': a form of private law that serves not only to safeguard individual autonomy, but also to structure the internal market in line with political and economic objectives [43]. Yet, as cautioned by Namysłowska, this evolution risks weakening the foundational principles of consumer law, such as fairness and professional diligence, by subordinating them to broader market logics [44].

That said, Section 4 DSA does not stand alone in protecting consumers who engage in commercial transactions on social media. In fact, social media commerce also falls under the scope of EU consumer laws, particularly the CRD and UCPD [26]. Similarly to the DSA, these legal instruments do not explicitly address this phenomenon, but impose a number of obligations on social media platforms when they act as online marketplaces (see Section 3.1 above) [4]. Imposing duties on online intermediaries marks a clear shift from the original logic of EU consumer law, initially designed to protect consumers (i.e. natural person who appears in the market without any profit-making intentions) in their 'bipolar interactions' with traders (i.e. natural or legal person acting for professional purposes) [45]. Over time, however, it has evolved into a legal field which also imposes consumer protection obligations on online intermediaries, due to their pivotal role in facilitating commercial transactions. This trend started with the adoption of the Modernisation Directive which introduced several provisions specifically applicable to online marketplaces [46], and has been since reinforced by the Court of Justice of the European Union (CJEU) in its case law. In the *Tiketa* case, for instance, it confirmed that online intermediaries can bear consumer protection obligations under the CRD [47]. The DSA further contributes to this trend by introducing consumer protection rules tailored to online platforms, thereby moving beyond the traditional binary relation between consumers and traders [48].

The EU legal framework applicable to social commerce is therefore highly fragmented, with consumer protection rules arising from sectoral (e.g. CRD, UCPD) and non-sectoral regulation (e.g. DSA) [26]. All of these frameworks aim to ensure that consumers are treated fairly, but their coexistence raises important questions about how they interact – a concern that was also voiced by Member States during the adoption of the DSA [49]. More specifically, it remains unclear to what extent these legal regimes complement, overlap with, or potentially contradict one another in regulating online intermediaries, including social marketplaces. Article 2(4) DSA addresses (or at least, tries to address) this issue by clarifying that *"this Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services",* and point (f) provides consumer protection as an example of legal acts. Essentially, this 'without prejudice' clause entails that the DSA, based on a horizontal approach, should be consistent with and should leave unaffected other areas of law [49]. In this context, the following sub-sections take a closer look at how the provisions set out in Section 4 DSA apply to social marketplaces, with a particular emphasis on their interaction with existing consumer protection rules.

#### 3.2.1. Article 30 DSA on traceability of traders

Under Article 30(1) DSA, 'online platforms allowing consumers to conclude distance contracts with traders' must obtain information from traders before allowing them to use their e-commerce services. Such information essentially concerns the legal status and identity of traders, including their name, their payment account details, and a copy of their identification document. The wording of this 'know-your-business-customer' suggests that not all third-party sellers must provide such information, but only those legally qualifying as traders. In this sense, a critical aspect in applying Article 30 DSA revolves around identifying who, among third-party sellers on social marketplaces, is considered a trader.

It is precisely in this type of situation that the interaction between the DSA and sectoral regulation, including the EU consumer *acquis,* becomes relevant. Legal instruments, such as the CRD and UCPD, impose related yet distinct obligations on online intermediaries regarding the distinction between third-party sellers and traders. Articles 6a(1)(b) CRD and 7 (4)(f) UCPD require online marketplaces to inform consumers whether the third-party offering the product or service is a trader or not, based on a declaration of that third-party. Although this self-declaration is a useful indication of the seller's status, it is not decisive from a legal standpoint and does not replace the qualification of a trader under the law [31]. Article 3(f) DSA defines a trader as *"any natural person, or any legal person irrespective of whether it is privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession"* [50]. As confirmed on multiple occasions by the CJEU, the notion of 'trader' is functional [51]: determining if a third-party seller on a social marketplace falls within its meaning must be done on a case-by-case basis. And to do so, national courts must take into account a list of non-exclusive and non-exhaustive criteria developed in the *Kamenova* case [52].

Determining whether a user qualifies as a trader is particularly challenging in the context of social marketplaces. Unlike traditional e-commerce platforms, where sellers are typically established professionals, users on social media often engage in mixed-purpose activities. They may use the same account to browse content and interact socially with others, while promoting or selling goods and services – making it difficult to assess whether they act as consumers or traders [53]. This ambiguity is acknowledged in Recital 17 CRD, clarifying that a natural person may still be considered a consumer in such circumstances *"if the trade purpose is so limited as not to be predominant in the overall context of the contract"*. The CJEU has echoed this reasoning in the *YYY* case, confirming that this classification depends on the dominant purpose of the activity [54]. In practice, this means that even individuals engaged in occasional sales or promotions on social marketplaces may still retain their consumer status – unless the professional aspect outweighs the personal one. These grey areas have led to the emergence of the so-called *prosumer:* a natural person who both consumes and produces, often in semi-professional ways that escape straightforward legal categorisation [55].

Influencers, also referred as content creators [56], exemplify this ambiguity, as their dual role in consuming and promoting content often places them at the intersection of consumers and traders [57]. In its

guidance on the application of the UCPD, the European Commission suggests that content creators who *frequently* conduct promotional activities towards consumers on their social media accounts are likely to be classified as traders, irrespective of their audience size [31]. Still, this determination must ultimately be made by national courts on a case-by-case basis, drawing on the functional definition of trader and the non-exhaustive set of criteria developed in the *Kamenova* case [52]. The informal and hybrid nature of social marketplaces therefore challenges the binary classification consumer-trader underpinning EU consumer law – originally designed for more traditional and structured commercial environments (see Section 3.2 above). This, in turn, complicates the application of Article 30 DSA which relies on the same binary distinction to trigger platform obligations.

Faced with this legal uncertainty, social marketplaces should therefore primarily rely on the self-declaration made by third-party sellers on their status as traders, as requested under Articles 6a(1)(b) CRD and 7(4)(f) UCPD, to comply with Article 30 DSA. In case third-party sellers declare that they are not traders, social marketplaces must inform consumers about the non-applicability of EU consumer protection laws to the contract [58]. Conversely, if third-party sellers consider themselves as traders, they fall within the scope of Article 30 DSA and must provide the information mentioned therein to social marketplaces. In the latter scenario, platforms must make best efforts to verify the reliability and completeness of such information, according to Article 30(2) DSA. Interestingly, this due diligence obligation does not exist yet in the EU consumer *acquis*. However, what could have been a valuable opportunity to enhance consumer protection was in reality a missed chance to establish a robust and uniform standard across platforms. The DSA fails to clarify what is meant by 'best efforts', which creates a challenge in setting a clear threshold for compliance. What is clear, however, is that verifying the information provided by traders should not lead to a general monitoring or an active fact-finding obligation for social marketplaces, as prohibited under Article 8 DSA [59].

#### 3.2.2. Article 31 DSA on compliance by design

Article 31(1) DSA requires 'online platforms allowing consumers to conclude distance contracts with traders' to design and organize their interface in a way that enables traders to comply with their own legal duties. I argue that this compliance-by-design provision does not bring anything revolutionary to the consumer protection landscape. Instead, it codifies an existing (although implied) obligation arising from the CRD and UCPD.

To begin with, the obligation laid down in Article 31(1) DSA already implicitly stemmed from the disclosure duties established in the CRD for distance contracts. More specifically, Article 6(1) CRD requires traders to provide pre-contractual information to consumers about their products or services. However, as traders heavily rely on the affordances of social marketplaces, they might encounter technical limits if the platform does not offer sufficient space to comply with this obligation. Consequently, as argued by Cauffman and Goanta, social media platforms already had an implicit obligation under the CRD to design and organize their online interface in order to enable traders to fulfil their disclosure duties [60]. When providing pre-contractual information to consumers, traders must also comply with the formal requirements applicable to distance contracts, laid down in Article 8 CRD. Interestingly, Article 8(4) CRD acknowledges that traders using distance communication (e.g. social media) may have limited space to provide information, and specifies the essential details to disclose in these circumstances [61]. At the same time, Article 31(2) DSA lists the information that social marketplaces must *at least* enable traders to provide while designing and organizing their online interface [62]. What is interesting is that the information mentioned in the CRD and the DSA do not entirely overlap. Article 8(4) CRD prioritises information directly relevant to the contractual decision of consumers (e.g. price, right of withdrawal), whereas Article 31(2) DSA focuses on trader traceability and product identification. This situation leads to a discrepancy in the minimum standard between what traders must disclose and what platforms must facilitate.

Similarly, 'online platforms allowing consumers to conclude distance contracts' were also implicitly required under the UCPD to comply with the obligation found in Article 31(1) DSA based on two grounds. First, Article 7(4) UCPD establishes a list of pre-contractual information, similar to Article 6(1) CRD, that traders must provide to consumers in case of an invitation to purchase. Second, these platforms were also required to design and organize their interface in a specific manner due to their 'professional diligence' obligations under Article 5(1) UCPD [63]. In its guidance on the application of the UCPD, the European Commission states that online platforms, as part of their professional diligence, should take appropriate measures to allow traders to comply with their consumer law obligations [31]. These measures may include designing *"their interfaces in a way that enables third party traders to present information to platform users, especially information required by Articles 6 CRD and 7(4) UCPD"* [31]. In this way, Article 31 DSA formalises an obligation that already existed under the EU consumer *acquis*, using almost the exact same wording as the European Commission in its guidance on the application of the UCPD.

Traditional e-commerce platforms, such as Amazon or eBay, have long adapted their online interfaces to comply with EU consumer law, offering templates for product listings, seller information, return policies, and other mandated disclosures. Social marketplaces, by contrast, have yet to achieve comparable levels of compliance. Formal social marketplaces, such as TikTok Shop, do provide some technical infrastructure for traders to input product details. But these efforts remain limited: information about the trader's identity is not prominently displayed at the point of transaction, but is typically accessible via their profile, often confined in the bio section. Informal social marketplaces offer even less support to traders using their e-commerce features, as they lack a structured interface for displaying pre-contractual information. Although traders can include this information on their own websites accessed through in-app browsers, Article 31(2) DSA requires platforms to *actively* design and organize their interface in a way that makes such information directly accessible on the platform itself. I therefore argue that merely redirecting consumers to external pages does not fulfil this obligation, nor does it ensure the level of visibility and clarity envisioned by the DSA.

Yet beyond these differences lies a more fundamental issue. The compliance-by-design obligation set out in Article 31 DSA presumes that platform architectures are sufficiently neutral and adaptable to support legal compliance – an assumption that does not hold true for social media platforms. Article 31 DSA imposes a technical obligation on online platforms to enable traders to comply with their own legal duties, suggesting that interface design can effectively be adapted to support such compliance. However, this overlooks a crucial point: social media platforms are structurally optimized for conflicting objectives, such as persuasive design and attention capture [64]. Their core architecture is designed to exploit the vulnerabilities of users [65], rather than to support meaningful transparency in online transactions. Social media interfaces are built around a logic of entertainment and emotional immersion [66], not one of standardization and legal certainty. Even when e-commerce features are added, they remain embedded in interfaces engineered for frictionless scrolling and passive content consumption [67], leaving little room for structural transparency under EU law.

#### 3.2.3. Article 32 DSA on right to information

Under Article 32(1) DSA, 'online platforms allowing consumers to conclude distance contracts with traders' are required to notify consumers when they become aware that those consumers have purchased an illegal product or service offered through their services. The notification must include information about the illegal nature of the product or service, the identity of the trader, and any relevant means of redress. Importantly, this obligation applies only to transactions concluded within six months prior to the platform becoming aware of the illegal

activity.

Article 32(1) DSA operates under the assumption that these platforms can identify which consumers have made a purchase through their services and have their contact details to issue the required notifications. For formal social marketplaces, this assumption holds true: the entire transactional process, including payment processing, is managed by the platform, which thereby retains the necessary data to trace individual purchasers. However, this level of data access is not guaranteed for informal social marketplaces. As previously discussed (see Section 2.2.2 above), a defining feature of informal social marketplaces is that they do not handle payments directly. Instead, they redirect consumers via their in-app browsers to the third-party seller's website, where the checkout process occurs. Once consumers are redirected on these external websites, informal social marketplaces have *in principle* no visibility over whether a transaction was completed, nor do they have the information needed to contact the consumer involved. For the purposes of Article 32 (1) DSA, this suggests that informal social marketplaces cannot determine which consumers have purchased an illegal good or product through their services, and therefore cannot notify them accordingly.

However, reality is different as shown by multiple studies conducted by Felix Krause. His research revealed that social media platforms can track activities on external websites hosted on their in-app browsers, without obtaining consent from users or website providers [35]. For instance, TikTok can record every tap on the screen and keyboard input when users interact with the trader's website, including sensitive data such as passwords or credit card information [68]. While this indicates that informal social marketplaces have the technical capacity to detect when a transaction occurs between a trader and a consumer, it remains uncertain whether data collected through their in-app browsers should be used to comply with Article 32(1) DSA. Using such information would raise significant privacy concerns and could expose social media companies to scrutiny from data protection authorities. Interestingly, social marketplaces publicly present their in-app browsers in far more neutral or even protective terms. According to Meta, its in-app browser enables *"a safe, convenient, and reliable experience for people and businesses"*, while detecting *"attacks from bad actors, like when a scammer tried to redirect your customer to a malicious site"* [22]. Meanwhile, TikTok has admitted to monitoring user interactions, such as key presses and click events, on third-party websites accessed through its in-app browser. However, it claimed that this data was used only *"for debugging, troubleshooting and performance monitoring of [user] experience, like checking how quickly a page loads or whether it crashes"* [69]. This explanation did not convince all users, leading some to file lawsuits in the United States against TikTok for illegal tracking of user behavior [70]. Given these privacy concerns and ongoing legal scrutiny, it is unlikely that informal social marketplaces will rely on data collected through their in-app browser to comply with Article 32(1) DSA.

As a result, they would automatically fall under the scope of Article 32(2) DSA. This provision applies when platforms do not have the contact details of consumers who purchased an illegal product or service through their services. In such cases, social marketplaces must make publicly and easily accessible on their interfaces the information mentioned in Article 32(1) DSA. From a consumer protection perspective, this type of public disclosure serves an important function: they can empower consumers to make better-informed choices and encourage online platforms to screen traders more carefully. Yet the impact of Article 32(2) DSA on consumer protection may be limited for two reasons. First, these public disclosures directly conflict with the commercial interests of social media companies, as they risk damaging the reputation of the platform and decrease user engagement. Frequent disclosures about illegal products may erode consumer trust in social marketplaces, discouraging further transactions, while simultaneously deterring advertisers and traders to post their offers due to brand safety concerns [71]. In competitive digital markets where user attention [64] and public perception are paramount [72], the reputational costs attached to public disclosures can therefore create disincentives for social marketplaces to comply. Second, enforcement authorities may lack the tools to verify whether a disclosure obligation has been triggered under Article 32(2) DSA. Unlike individual notifications under Article 32(1) DSA, which can (in principle) be audited through transaction records, public disclosures leave no clear trace if omitted – particularly on informal social marketplaces that do not process payments and therefore, have no legally collected evidence of completed transactions. Additionally, the DSA does not specify how long these disclosures must remain visible and accessible on platform interfaces, which further complicates compliance over time. These gaps may limit enforcement and leave consumers unaware of their exposure to illegal products or services on social marketplaces, weakening the very transparency and redress mechanisms that Article 32(2) DSA is meant to provide.

## 4. Shortcomings in the DSA's approach to consumer protection in social media commerce

In this paper, I analysed how the DSA protects consumers engaging in commercial transactions on social marketplaces. While the legal framework applicable traditional online marketplaces is well established, the same clarity does not extend to social commerce: a new form of online shopping occurring on platforms whose business models initially relied on social networking. The analysis highlighted that the DSA imposes obligations on social marketplaces that are directly relevant to consumer protection. These obligations are set out in Section 4 DSA, which applies to 'online platforms allowing consumers to conclude distance contracts with traders'. And as previously argued (see Section 3.1 above), social media platforms with e-commerce features, what I refer to as *social marketplaces,* fall into this category of online platforms and must therefore comply with these obligations.

However, integrating these DSA obligations into the broader EU consumer law framework raises important questions of legal coherence. In the previous section, I examined how the provisions laid down in Section 4 DSA interact with existing legal instruments of the EU consumer *acquis,* such as the CRD and UCPD, in the context of social media commerce. Building on that analysis, I identify three shortcomings in the DSA's approach to tackle social commerce from a consumer protection perspective. These concern not only the adequacy and clarity of the obligations introduced by the DSA itself, but also the challenges of interpreting and applying them consistently alongside pre-existing consumer protection rules.

### 4.1. Regulatory complexity

The first shortcoming concerns the regulatory complexity of the consumer protection landscape applicable to social media commerce, resulting from the interplay between the DSA and the EU consumer *acquis.* As previously discussed (see Section 3.2 above), the obligations laid down in Section 4 DSA apply in conjunction with existing consumer rules, which also impose duties on online intermediaries such as social marketplaces. Article 2(4)(f) DSA affirms that the DSA is 'without prejudice' to other Union legal acts, and is therefore meant to leave consumer protection laws unaffected and consistent with them [49]. However, the interaction between these frameworks reveals a different picture – one marked by regulatory complexity. For instance, the analysis in Section 3.2.2 identified one point of tension between Article 31 (2) DSA, which sets the information that platforms must at least make technically possible for traders to provide through their interface, and Article 8(4) CRD, which specifies the minimum information that traders must disclose to consumers. In this scenario, the obligations under the CRD could be considered *lex specialis* and hence, override the provisions of the DSA [73].

Even when legal texts are not in formal contradiction, regulatory complexity remains a concern. Contextualising the newly introduced obligations of the DSA with existing consumer protection laws proves to be a challenging legal exercise. A key example of this complexity is the

interplay between Article 30 DSA, which requires online marketplaces to collect information from traders, and Articles 6a(1)(b) CRD and 7(4)(f) UCPD, according to which these platforms must inform consumers about the legal status of traders (see Section 3.2.1 above). Looking ahead, the complexity of the regulatory framework applicable to social media commerce might increase. According to the study supporting the Digital Fairness Fitness Check, the European Commission should consider adopting consumer protection rules specifically tailored to social commerce [26]. This recommendation is based on the concern that the absence of clear rules weakens both the application and enforcement of consumer protection on social marketplaces, as discussed in the following sub-sections [26].

### 4.2. Interpretative ambiguity

The second shortcoming relates to the difficulty of interpreting and applying the DSA provisions to industries and practices they were not envisaged for at the time of drafting, namely social marketplaces. The obligations laid down in Section 4 DSA, along with those contained in the CRD and UCPD, were drafted for traditional e-commerce platforms (e.g. eBay, Amazon), where consumer transactions are clearly delineated and actors easily identifiable. This clarity does not extend to social marketplaces, which are dynamic user-generated ecosystems that blur the lines between social interaction and commercial activity. The fact that the DSA was not designed with such hybrid environments in mind is evident from Recital 13 DSA, which treats 'social networks' and 'online platforms allowing consumers to conclude distance contracts' as two distinct categories of online platforms (see Section 3.2 above). Yet, in practice, an increasing number of social media platforms serve both functions simultaneously. By the time the DSA was adopted, platforms like Instagram, TikTok, and Pinterest had already introduced e-commerce features into their services. Failing to account for this convergence is a missed opportunity to address the realities of digital markets as they currently operate [26].

Consequently, it becomes challenging to determine how Section 4 DSA and related consumer protection obligations apply to social marketplaces. For instance, should a 'Shop Now' button beneath a TikTok video trigger the same compliance-by-design obligations under Article 31 DSA as a traditional product listing on Amazon? Is the requirement to inform consumers about the identity of traders under Article 30 DSA, in conjunction with Articles 6a(1)(b) CRD and 7(4)(f) UCPD, satisfied if that information is only accessible via the seller's profile? Similarly, what obligations arise when purchases are made through an in-app browser that redirects consumers to an external website? Without precise interpretative guidance (rather than new legislation, given the existing regulatory complexity described above), and targeted enforcement strategies adapted to the distinctive features of social commerce (see Section 4.3 below), the current legal framework risks falling short of delivering effective and meaningful consumer protection.

### 4.3. Enforcement gap

The third shortcoming relates to the challenge of enforcing the DSA in the context of social media commerce. While Section 4 DSA does introduce new obligations designed to increase platform transparency and consumer protection, these obligations have not yet been enforced in relation to social marketplaces. This observation is based on the current lack of public evidence showing meaningful enforcement of Section 4 DSA in the context of social media commerce. To date, enforcement efforts under the DSA have been largely directed at traditional e-commerce platforms, where consumer protection issues (e.g. misleading information, deceptive product labels, sale of illegal products) continue to surface [74]. Although the precise reasons for this enforcement gap are difficult to determine, a number of structural and institutional barriers may help explain why social marketplaces have so far escaped regulatory scrutiny.

First, this lack of enforcement can be attributed to the limited and uneven roll-out of e-commerce features on social media platforms [4]. Until recently, only informal social marketplaces were available in the EU (see Section 2.2.2 above), making commercial activity less visible to authorities and less likely to prompt enforcement actions. Second, applying existing legal frameworks to social media commerce is not straightforward. The provisions in Section 4 DSA, together with the EU consumer *acquis,* were not designed to regulate online platforms where social interaction and commercial activity coexist in fluid ways (i.e. social marketplaces) [26]. As a result, enforcement is hindered *not* by the absence of rules, but by the challenge of understanding how they apply to evolving platform dynamics – what I referred to in the previous sub-section as interpretive ambiguity. A final obstacle to enforcement is the unavailability of reliable data. Article 40(1)-(3) DSA grants Digital Services Coordinators and the European Commission access to data from VLOPs to monitor compliance. However, this provision might fall short in the context of social commerce, particularly for informal social marketplaces that do not process payments. As transactions occur off-platform, there may be no *lawfully* collected data to confirm that a purchase occurred through their services. Without such data, monitoring the obligations set out in Section 4 DSA, such as Article 32 DSA on the right to information (see Section 3.2.3 above), becomes nearly impossible.

One should also note that, since the adoption of the DSA, enforcement responsibilities related to consumer protection on online platforms – including social marketplaces – are shared across a broader network of actors (e.g. European Commission, Digital Services Coordinators). This marks a significant shift from traditional EU consumer law, where enforcement has primarily rested within national courts and administrative bodies [4]. Coordination will therefore be critical to ensuring legal coherence, in particular when the DSA intersects with existing instruments such as the CRD and UCPD [75].

## 5. Conclusion

This article examined how the DSA protects consumers in relation to social commerce, and what specific obligations it imposes on, what I call, social marketplaces (i.e. social media platforms with e-commerce features) to increase transparency in online transactions. First, I shed light on the concept of social media commerce, defined in this article as the direct selling of goods and services through social media platforms. I then described how, at the time of the writing, social media platforms engage in e-commerce in the EU, distinguishing between formal and informal social marketplaces. Building on this foundation, I analysed how the DSA, and more specifically Section 4 DSA, applies to these emerging practices, and explored its interplay with EU consumer laws, such as the CRD and UCPD.

The analysis revealed three shortcomings in the DSA's approach to tackle social media commerce from a consumer protection perspective. First, it introduces regulatory complexity, by layering new obligations applicable to social marketplaces onto existing consumer laws – an issue that is likely to increase in light of the study supporting the Digital Fairness Fitness Check, suggesting the European Commission to adopt rules specifically applicable to social commerce [26]. Second, the DSA suffers from interpretative ambiguity, as the provisions laid down in Section 4 DSA were not designed having social marketplaces in mind. Third, enforcement actions targeting social media commerce are still lacking, due to the complexity this phenomenon and the involvement of a broad network of enforcement actors.

While the DSA holds promise, its effectiveness will ultimately depend on how national authorities and the European Commission apply its provisions to social marketplaces – platforms that were not the initial focus of the Regulation. Rather than introducing new rules, the priority should be to clarify the legal interaction between legal instruments, to interpret existing provisions in light of new platform practices, and to ensure coordinated enforcement across relevant actors in order to

deliver meaningful consumer protection on social marketplaces.

## Funding sources

This work was supported by the Luxembourg National Research Fund PRIDE19/14268506.

## Declaration of competing interest

The author declares no conflict of interests.

## Acknowledgments

The author would like to thank (in alphabetical order) Taylor Annabell, Elettra Bietti, Catalina Goanta, Rachel Griffin, Tamara Perišin and Elise Poillot for their generous feedback and support throughout the writing process. The author is also grateful to the anonymous reviewers for their comments and suggestions, which have greatly improved the article.

## Data availability

No data was used for the research described in the article.

## References

[1] Facebook, Introducing Marketplace: Buy and Sell With Your Local Community. https://about.fb.com/news/2016/10/introducing-marketplace-buy-and-sell-with-your-local-community/, 2016 (accessed 4 September 2024).
[2] TikTok, Video Shopping Ads: Supercharge Product Sales. https://www.tiktok.com/business/en-US/solutions/ecommerce/shoppingads?ab_version=control, 2022 (accessed 4 September 2024).
[3] Instagram, How to Tag Products on Instagram Feed Posts. https://business.instagram.com/blog/instagram-shopping-product-tags-customers, 2021 (accessed 12 September 2024).
[4] European Commission, Commission Staff Working Document Fitness Check of EU consumer law on digital fairness [2024]SWD(2024) 230 final.
[5] Big News Network, The Future of E-Commerce: How TikTok Live Selling and Shopify Mobile App are Revolutionizing the Live Selling Platform. https://www.bignewsnetwork.com/news/274565171/the-future-of-e-commerce-how-tiktok-live-selling-and-shopify-mobile-app-are-revolutionizing-the-live-selling-platform#google_vignette, 2024 (accessed 12 September 2024); FenixCommerce, How Social Commerce Is Growing and Why It Will Shape E-Commerce in the Future. https://fenixcommerce.com/how-social-commerce-is-growing-and-why-it-will-shape-e-commerce-in-the-future/, 2024 (accessed 12 September 2024).
[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022]OJ L277 (Digital Services Act).
[7] Busalim A, Razak Che Hussin A. Understanding Social Commerce: A Systematic Literature Review and Directions for Future Research. Int. J. Inf. Manag. 2016;36:1075–88. https://doi.org/10.1016/j.ijinfomgt.2016.06.005.
[8] L. Zhou, P. Zhang, H. Zimmermann, Social Commerce Research: An Integrated View, Electron. Commer. Res. Appl. 12(2) (2013) 61-68. https://doi.org/10.1016/j.elerap.2013.02.003; X. Lin, Y. Li, X. Wang, Social Commerce Research: Definition, Research Themes and the Trends, Int. J. Inf. Manag. 37(3) (2017) 190-201. https://doi.org/10.1016/j.ijinfomgt.2016.06.006; E. Akar, B. Topçu, An Examination of the Factors Influencing Consumers' Attitudes Toward Social Media Marketing, J. Internet Commer. 10 (2011) 35-67. https://doi-org.proxy.bnl.lu/10.1080/15332861.2011.558456; N. Hajli, Social Commerce Constructs and Consumers' Intention to Buy, Int. J. Inf. Manag. 35 (2015) 183-191. https://doi.org/10.1016/j.ijinfomgt.2014.12.005.
[9] Kim D. Under What Conditions Will Social Commerce Business Models Survive? Electron. Commer. Res. Appl. 2013;12(2):69–77. https://doi.org/10.1016/j.elerap.2012.12.002.
[10] Curty R, Zhang P. Social Commerce: Looking Back and Forward. Proc. Am. Soc. Inf. Sci. Technol. 2011;48(1):1–10. https://doi.org/10.1002/meet.2011.14504801096.
[11] Y.-C. Wu, J.-P. Shen, C.-L. Chang, Electronic Service Quality of Facebook Social Commerce and Collaborative Learning, Comput. Hum. Behav. 51 (2015) 1395-1402. https://doi.org/10.1016/j.chb.2014.10.001; Z. Huang, M. Benyoucef, From E-Commerce to Social Commerce: A Close Look at Design Features, Electron. Commer. Res. Appl. 12 (2013) 246-259. https://doi.org/10.1016/j.elerap.2012.12.003.
[12] Constantinides E, Romero L, Boria M. Social Media: A New Frontier for Retailers? In: Swoboda B, Morschett D, Rudolph T, Schnedlitz P, Schramm-Klein H, editors. European Retail Research. Wiesbaden: Gabler Verlag; 2008. p. 1–28.
[13] Sturiale L, Scuderi A. Evaluation of Social Media Actions for the Agrifood System. Procedia Technol 2013;8:200–9. https://doi.org/10.1016/j.protcy.2013.11.028.
[14] Liang T-P, Turban E. Introduction to the Special Issue Social Commerce: A Research Framework for Social commerce. Int. J. Electron. Commerce 2011;16(2):5–14. https://doi.org/10.2753/JEC1086-4415160201.
[15] C. Riefa, Consumer Protection on Social Media Platforms: Tackling the Challenges of Social Commerce, in T. Synodinou, Ph. Jougleux, C. Markou, Th. Prastitou (Eds.), EU Internet Law in the Digital Era, Springer Cham, Switzerland, 2017, pp. 321-345; C. Goanta, The New Social Media: Contracts, Consumers, and Chaos, Iowa L. Rev. Online 108 (2023) 118-130. https://ilr.law.uiowa.edu/volume-108-response-pieces/2023/05/new-social-media-contracts-consumers-and-chaos.
[16] Meta, Shopping on Facebook. https://www.facebook.com/business/news/shopping-on-facebook, 2015 (accessed 4 September 2024); V Luckerson, Here's Why 'Buy Buttons' Are Invading the Internet'. https://time.com/4075560/buy-button-facebook-youtube-pinterest/, 2015 (accessed 4 September 2024).
[17] Martínez-López F, Li Y, Su W, Feng C. To Have or Have Not: Buy Buttons on Social Platforms. J. Bus. Res. 2019;105:33–48. https://doi.org/10.1016/j.jbusres.2019.07.029.
[18] Interestingly, this convergence is also operating the other way around. While social media platforms are integrating e-commerce, traditional online marketplaces (e.g. Amazon) are also introducing social networking features into their services Zhao L, Yalin A, West E. E-Commerce Goes Social: The Rise of Livestreaming as a Hybrid Promotional Form. In: West E, McAllister MP, editors. The Routledge Companion to Advertising and Promotional Culture. New York: Routledge; 2023. p. 347–59.
[19] West E. Buy Now: How Amazon Branded Convenience and Normalized Monopoly. Cambridge: MIT Press; 2022.
[20] TikTok, TikTok Shop: Always Moving Your Business Forward. https://business.tiktokshop.com/us/seller, (accessed 15 May 2025).
[21] D. Katanich, TikTok Launches Online Shopping in Spain and Ireland. https://www.euronews.com/business/2024/12/10/tiktok-launches-online-shopping-in-spain-and-ireland, 2024 (accessed 15 May 2024). As of this writing, TikTok Shop is available in five EU Member States: Spain, Ireland, France, Germany, and Italy.
[22] Meta, About the In-App Browser for Facebook and Instagram, https://www.facebook.com/business/help/206578174518231, (accessed 14 September 2024).
[23] Article 1(1) DSA, together with Recital 4 of the Preamble to the DSA.
[24] B. Duivenvoorde, C. Goanta, The Regulation of Digital Advertising Under the DSA: A Critical Assessment, Comput. Law Secur. Rev. 51 (2023) 1-14. https://doi.org/10.1016/j.clsr.2023.105870; P. Wolters, F. Zuiderveen Borgesius, The EU Digital Services Act: What Does it Mean For Online Advertising and Adtech? Int. J. Law Inf. Technol. 33 (2025). https://doi.org/10.1093/ijlit/eaaf004; E. Izyumenko, M. Senftleben, N. Schutte, E. Smit, G. van Noort, L. van Velzen, Online Behavioural Advertising, Consumer Empowerement and Fair Competition: Are the DSA Transparency Obligations the Right Answer? J. Eur. Consum. Market Law 14(2) (2025) 46-59.
[25] Duivenvoorde B. The Regulation of Online Marketplaces under the Unfair Commercial Practices Directive, the E-Commerce Directive and the Digital Services Act. J. Eur. Consum. Market Law 2022;11(2):43–52.
[26] Directorate-General for Justice and Consumers, Study to support the fitness check of EU consumer law on digital fairness and report on the application of the Modernisation Directive [2024]Final Report – Part 2.
[27] The notion of distance contract is defined in Article 2(7) CRD as "any contract concluded between the trader and the consumer under an organized distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded". According to this definition, contracts concluded between users through the intermediary of social media platforms clearly fall under this category of contract.
[28] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011]OJ L304 (Consumer Rights Directive).
[29] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005]OJ L149 (Unfair Commercial Practices Directive).
[30] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328 (Modernisation Directive).
[31] European Commission, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (C/2021/9320) [2021]OJ C526.
[32] Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC [2018]OJ LI60 (Geo-Blocking Regulation).
[33] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the

enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 [2017]OJ L345 (Consumer Protection Cooperation Regulation).
[34] Article 3(m) DSA offers a slightly different definition of the term 'online interface', describing it as *"any software, including a website or a part thereof, and applications, including mobile applications"*. Articles 2(16) of the Geo-Blocking Regulation and 3 (15) of the Consumer Protection Cooperation Regulation are used in this article because Recital 25 of the Modernisation Directive specifically relies on these provisions when using the term 'online interface'.
[35] F Krause, IOS Privacy: Instagram and Facebook can track anything you do on any website in their in-app browser. https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser, 2022 (accessed 4 September 2024).
[36] C. Goanta, Now What: Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising, https://verfassungsblog.de/dsa-now-what/, 2022 (accessed 15 September 2024).
[37] Recital 1 DSA also mentions "online social networks *and* (emphasis added) online platforms allowing consumers to conclude distance contracts with traders".
[38] Case C-162/97 *Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn* [1998]ECLI:EU:C:1998:554, para 54; T. Klimas, J. Vaiciukaite, The Law of Recitals in European Community Legislation, J. Int'l & Comp. L. 61 (2008) 61-94.
[39] P. Leerssen, An End to Shadow Banning? Transparency Rights in the Digital Services Act Between Content Moderation and Curation, Comput. Law Secur. Rev. 48 (2023) 1-13. https://doi.org/10.1016/j.clsr.2023.105790; J. P. Quintais, N. Appelman, R. Fathaigh, Using Terms and Conditions to Apply Fundamental Rights to Content Moderation, Ger. Law J. 24(5) (2023) 881-911. https://doi.org/10.1017/glj.2023.53; J. van de Kerkhof, Article 22 Digital Services Act: Building Trust with Trusted Flaggers, Internet Policy Rev. 14(1) (2025). https://doi.org/10.14763/2025.1.1828.
[40] Article 1(1) DSA, together Recital 3 of the Preamble to the DSA.
[41] Consolidated version of the Treaty on the Functioning of the European Union [2007]OJ C326; E. Poillot, Droit européen de la consommation, in: D. Fenouillet (Ed.), Droit de la consommation, Dalloz Action, Paris, 2021, pp. 49-73.
[42] Schulte-Nölke H. The EU Digital Services Act and EU Consumer Law. In: De Franceschi A, Schulze R, editors. Harmonizing Digital Contract Law: The Impact of EU Directives 2019/770 and 2019/771 and the Regulation of Online Platforms. Baden-Baden: Beck/Nomos/Hart; 2019. p. 705–13.
[43] Micklitz H-W. The Visible Hand of European Regulatory Private Law – The Transformation of European Private Law from Autonomy to Functionalism in Competition and Regulation. Yearbook of European Law 2009;28(1):3–59. https://doi.org/10.1093/yel/28.1.3.
[44] Namysłowska M. The Silent Death of EU Consumer Law and Its Resilient Revival: Reinventing Consumer Protection Against Unfair Digital Commercial Practices. J. Consum. Policy 2025. https://doi.org/10.1007/s10603-025-09590-5.
[45] N. Reich, H-W. Micklitz, Economic Law, Consumer Interests, and EU Integration, in N. Reich, H-W. Micklitz, P. Rott and K. Tonner (Eds.), European Consumer Law, 2nd ed., Intersentia, Cambridge, 2014; G. Howells, T. Wilhelmsson, EC Consumer Law, Routledge, London, 1997; C. Busch, H. Schulte-Nölke, A. Wiemiórowska-Domagalska, F. Zoll, The Rise of the Platform Economy: A New Challenge for EU Consumer Law? J. Eur. Consum. Market Law 1 (2016) 3-10..
[46] Cauffman C. New EU Rules on Business-to-Consumer and Platform-to-Business Relationships. Maastricht J. Eur. Comp. Law 2019;26:469–88. https://doi.org/10.1177/1023263X19865835.
[47] Case C-536/20 *UAB 'Tiketa' v M. Š.* [2022]ECLI:EU:C:2022:112.
[48] F. de Elizalde, Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law, J. Consum. Policy 48(1) (2025). https://doi-org.proxy.bnl.lu/10.1007/s10603-025-09584-3; C. Busch, V. Mak, Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation, J. Eur. Consum. Market Law 10 (2021) 109-123. https://doi.org/10.2139/ssrn.3933675.
[49] Husovec M. Principles of the Digital Services Act. Oxford: Oxford University Press; 2024.
[50] It should be mentioned that EU law does not establish a single, uniform definition of the concept of trader. Instead, each legal instrument defines it according to its specific objectives.
[51] Case C-147/16 *Karel de Grote – Hogeschool Katholieke HogeschoolAntwerpenVZW v Susan Romy Jozef Kuijpers* [2018]ECLI:EU:C:2018:320, para 55; Case C-105/17 *Komisia za zahtita na potrebitelite v Evelina Kamenova* [2018]ECLI:EU:C:2018:378, para 35.
[52] Case C-105/17 *Komisia za zahtita na potrebitelite v Evelina Kamenova* [2018]ECLI:EU:C:2018:378, para 38.
[53] C. Riefa, L. Clausen, Towards Fairness in Digital Influencers' Marketing Practices, J. Eur. Consum. Market Law 8(2) (2019) 64-74; T. Annabell, L. Aade, C. Goanta, (Un)disclosed Brand Partnerships: How Platform Policies and Interfaces Shape Commercial Content for Influencers, Internet Policy Rev. 13(4) (2024). https://doi.org/10.14763/2024.4.1814.
[54] Case C-570/21 *YYY*. [2023]ECLI:EU:C:2023:456.
[55] A. Toffler, The Third Wave, Bantam Books, New York, 1980; V. Mak, Redefining Equality in European Contract Law: Protecting Consumer Interests in a Post-Consumer Society, Eur. Law Open 3(3) (2024) 561-586. https://doi.org/10.1017/elo.2024.42.
[56] S. Bishop, "Creator" and "influencer" aren't different jobs. Who does it serve to pretend they are? https://reallifemag.com/name-of-the-game/, 2021 (accessed 16 May 2025).
[57] Annabell T, Kelder T, van de Kerkhof J, Goanta C. Influencer as Individual and Trader: Exploring the Boundaries of Discrimination in Influencer Marketing from a Multidisciplinary Perspective. J. Media and Cult. Stud. 2025:1–16. https://doi.org/10.1080/10304312.2025.2518967.
[58] Article 6a(1)(c) CRD.
[59] Recital 74 DSA.
[60] Cauffman C, Goanta C. A New Order: The Digital Services Act and Consumer Protection. Euro. J. Risk. Regul. 2021;12(4):758–74. https://doi.org/10.1017/err.2021.8.
[61] Article 8(4) CRD requires traders to at least provide pre-contractual information regarding *"the main characteristics of the goods or services, the identity of the trader, the total price, the right of withdrawal, the duration of the contract and, if the contract is of indeterminate duration, the conditions for terminating the contract"*.
[62] Article 31(2) DSA requires the following information to be disclosed to consumers: "*(a) the information necessary for the clear and unambiguous identification of the products or the services promoted or offered to consumers located in the Union through the services of the providers; (b) any sign identifying the trader such as the trademark, symbol or logo; and (c) where applicable, the information concerning the labelling and marking in compliance with rules of applicable Union law on product safety and product compliance"*.
[63] Article 2(h) UCPD defines the concept of professional diligence as *"the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity"*.
[64] T. Wu, Blind Spot: The Attention Economy and the Law, Antitrust L. J. 82 (2018) 771-206; V. R. Bhargava, M. Velasquez, Ethics of the Attention Economy: The Problem of Social Media Addiction, Bus. Ethics Q. 31(3) (2021) 321-359. https://doi.org/10.1017/beq.2020.32; E. Bietti, The Data-Attention Imperative, Northeastern University School of Law Research Paper No. 473 (2024). https://doi.org/10.2139/ssrn.4729500.
[65] Helberger N, Sax M, Stryharz J, Micklitz H-W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. J. Consum. Policy 2022;45(2):175–200. https://doi.org/10.1007/s10603-021-09500-5.
[66] K. Wahl-Jorgensen, The Emotional Architecture of Social Media, in Z. Papacarissi (Ed.), A Networked Self and Platforms, Stories, Connections, Routledge, London, 2018, 78-93; A. Kramer, J. E. Guillory, J. T. Hancock, Experimental Evidence of Mass-Scale Emotion Contagion Through Social Networks, Proc. Natl. Acad. Sci. U. S. A. 111(24) (2014) 8788-8790. https://doi.org/10.1073/pnas.1320040111.
[67] D. Rozgonjuk, C. Sindermann, J. Elhai, A. Christensen, C. Montag, Associations Between Symptoms of Problematic Smartphone, Facebook, WhatsApp, and Instagram Use: An Item-Level Exploratory Graph Analysis Perspective, J. Behav. Addict. 9(3) (2020) 686-697. https://doi.org/10.1556/2006.2020.00036; C. Entrena-Serrano, Watch, Scroll, Repeat: How Interface Design Shapes Consumptive Curation Affordances on TikTok, Social Media + Society 11(3) (2025). https://doi.org/10.1177/20563051251358529.
[68] F Krause, IOS Privacy: Announcing InAppBrowser.com – see what JavaScript commands get injected through an in-app browser. https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser, 2022 (accessed 4 September 2024).
[69] TikTok, TikTok Truths: A new series on our privacy and data security practices. https://newsroom.tiktok.com/en-us/tiktok-truths-a-new-series-on-our-privacy-and-data-security-practices, 2023 (accessed 4 September 2024).
[70] Mehorter K. TikTok's In-App Web Browser Secretly Tracks Users. Class Action Claims 2022. https://www.classaction.org/blog/tiktoks-in-app-web-browser-secretly-tracks-users-class-action-claims (accessed 16 September 2024).
[71] Griffin R. From Brand Safety to Suitability: Advertisers in Platform Governance. Internet Policy Rev. 2023;12(3). https://doi.org/10.14763/2023.3.1716.
[72] T. Gillespie, The Politics of 'Platforms', New Media Soc. 12(3) (2010) 347-364. https://doi-org.proxy.bnl.lu/10.1177/1461444809342738; T. Gillespie, The Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media, Yale University Press, New Haven, 2018.
[73] It should be noted that this regulatory complexity is not exclusive to social marketplaces. Even in the context of traditional online marketplaces, the coexistence of rules under the DSA and the EU consumer *acquis* can create legal uncertainty. Yet this challenge may be more pronounced in the context of social media commerce, due to the blurred roles of actors and the hybrid nature of transaction flows on social marketplaces.
[74] European Commission, Commission Preliminary Finds Temu in Breach of the Digital Services Act in Relation to Illegal Products on its Platform. https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-temu-breach-digital-services-act-relation-illegal-products-its, 2025 (accessed 6 August 2025); European Commission, Commission and National Authorities Urge SHEIN to Respect EU Consumer Protection Laws, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1331, 2025 (accessed 6 August 2025).
[75] Durovic M. How to Remain Fit for the Digital Age: The Example of EU Consumer Law. J. Eur. Consum. Market Law 2024;13(6):246–55.