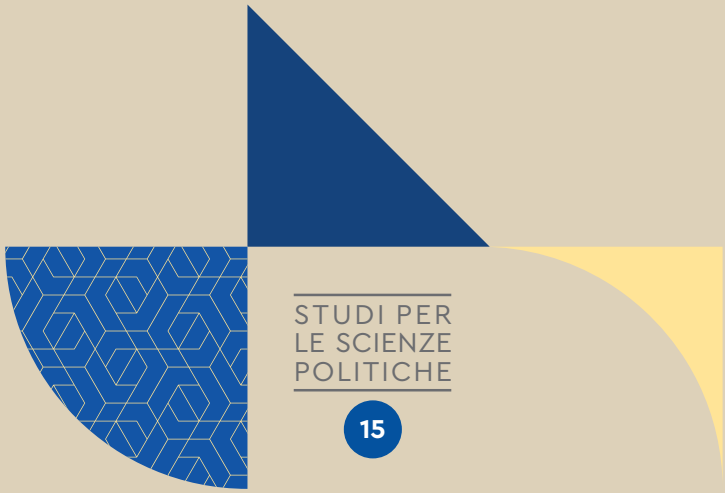
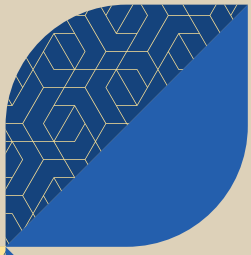


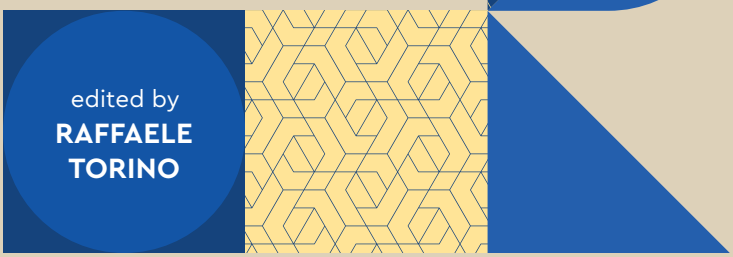
STUDI PER
LE SCIENZE
POLITICHE

15

DIGITAL CITIZENSHIP IN THE EUROPEAN UNION FRAMEWORK

POLITICAL, ECONOMIC, SOCIOLOGICAL, AND LEGAL ISSUES





edited by
RAFFAELE TORINO

Roma TrE-Press
2024

Raffaele Torino

The legal protection of the European Digital Consumer. An Introduction

Abstract: European consumer rights and interest protection policy represents one of the best examples of the added value that European integration brings to the daily lives of European citizens. The digitalization of consumer relations has led the European legislator to adopt numerous regulatory measures that strengthen consumer protection specifically in online consumption, within the broader context of European digital market regulation. This work serves as an introductory illustration of the numerous and innovative regulatory aspects that today protect the European digital consumer.

Keywords: Digital consumer – EU law – digital goods – social platforms – online market – personal data – geoblocking – artificial intelligence.

1. *The Digital Consumer*

Based on the European notion of a consumer as «any natural person who […] is acting for purposes which are outside his trade, business, craft, or profession» (Dir. 2011/83/EU, art. 2), the term 'digital consumer' can be defined and understood in various ways.

Firstly, if we want to adopt a legal approach based on the object of the act of consumption, the digital consumer is primarily someone who acquires a digital good or a digital service to satisfy a non-professional need of their own or of another person. In an interpretation that adopts a perspective related to the tool with which the act of consumption is carried out, a digital consumer can also be considered as someone who

uses digital means of communication (the Internet above all and the many possibilities it offers) to acquire –always as a consumer– non-digital goods or services, such as a book, food, clothing (but also digital goods and services). The first interpretation of 'digital consumer' also includes those who use specific digital services represented by access to (and use of) online platforms (primarily social platforms) and the publication (and enjoyment) of content (text, images, sounds) online.

In all cases, the advent of the phenomenon of digitalization (of goods or services, or the means of communication with consumer's contractual counterpart) necessitates a reconsideration of the protection that the legal system ensures for the interests and rights of the consumer.

Fully aware of this, within the framework of the progressive realization of the internal market provided for by Article 3 of the Treaty on European Union ('TEU') and Article 26 of the Treaty on the Functioning of the European Union ('TFEU') and the consumer protection policy established by Article 169 of the TFEU, the European Union has in recent years adopted a series of legislative acts that – according to the European Commission's plan set by the Communication of April 2018 significantly titled 'A New Deal for Consumers' – have progressively built a framework for the protection of the rights and interests of digital consumers within the context of the multi-level European legal system (resulting from the relationship between European sources, national legal systems, and European and national jurisprudence). This framework has made the aforementioned multi-level European legal system a legal system in this respect, as already happened with the broader consumer protection.

Having briefly outlined the legislative measures adopted by the European Union of specific interest to the digital consumer (section 2), this contribution aims to provide –without any claim to completeness – an introduction to some of the most innovative and/or problematic aspects in the protection of the interests and rights of digital consumers. Such introduction will briefly illustrate the protection framework for consumers of digital goods (section 3), draw attention to the debated issue of personal data of consumers as 'consideration' for digital goods or services (section 4), reconstruct the legal issues arising from the unbalanced relationship between Social Platforms and user-consumers (section 5), outline the new protections granted to consumers in online markets (section 6), summarize developments concerning the circulation of consumers' personal data outside the European Union (section 7) describe the new rules on online searches and reviews conducted by consumers (section 8), present the achievements reached at the European

level regarding the issues of portability and geo-blocking (section 9), list the consumer interest profiles in relation to the European Code of Electronic Communication (section 10), and, finally, highlight the perspectives opening up in relation to liability for damage arising from the use of artificial intelligence systems (section 11).

2. *The European Legal Framework*

The protection of the digital consumer at the European level (and consequently at the national level for the states participating in the European integration process) is rooted in the extensive body of legislation that the European Union (and, before it, the European Community) has progressively built since the mid-1980s.

In this context, central to the digital consumer protection have been, first and foremost, the directives that in recent decades have provided a uniform framework of protection regarding contracts entered into by consumers for the purchase –primarily at a distance– of movable goods (Directive 85/577/EEC, Directive 97/7/EC, Directive 1999/44/EC), the specific issue of unfair terms (Directive 93/13/EEC), electronic commerce (Directive 2001/31/EC), and unfair commercial practices (Directive 2005/29/EC).

Recently, a further set of conspicuous legislative measures have been introduced into this complex and articulated set of provisions (enhanced by the equally important case law of the Court of Justice of the European Union), representing a step ahead with respect to the specific protection of the digital consumer:

a) Directive (EU) 2018/1972 establishing the European Communications Code;
b) Directive (EU) 2019/770 concerning contracts for the supply of digital content and digital services;
c) Directive (EU) 2019/771 concerning contracts for the sale of goods;
d) Directive (EU) 2019/2161 regarding the better enforcement and modernization of Union consumer protection rules;
e) Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC ('Digital Services Act' or 'DSA').

To the list of the aforementioned measures, the General Data Protection Regulation (or GDPR) must undoubtedly be added. This regulation is a cornerstone for the protection of the digital consumer's data in a context where competition among companies regarding consumer choices increasingly relies on the data consumers spread in the real and digital world before, during, and after the act of consumption. Companies collect this data massively or acquire it from those who collect it, in a manner that may or may not be lawful, respecting the consumer's rights as the data subject interested in the correct and lawful processing of their personal data.

Furthermore, the rapid evolution of the digital world in which the digital consumer operates has compelled the European legislator to consider the phenomenon of artificial intelligence systems. In this regard, the reference is the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 ('AI Act') and the proposal of September 2022 for a Directive on non-contractual civil liability rules for artificial intelligence (AI Liability Directive).

For completeness, although not specifically aimed at protecting the rights and interests of consumers, it is also worth mentioning Regulation (EU) 2019/1150, which promotes fairness and transparency for business users of online intermediation services. This primarily refers to services that enable business users to offer goods or services to consumers. Improving the competitive environment among professional economic operators online will represent, albeit indirectly, an undoubted benefit for digital consumers.

Lastly, I believe it is worth noting that, in addition to the mandatory regulatory framework established by the European legislator, digital consumers undoubtedly benefit from the voluntary commitments made by companies. In this regard, I am particularly referring to the 'Consumer Protection Pledge' which sets out voluntary commitments of online platforms operating in the EU. It consists of two parts: the 'Product Safety Pledge' and the 'Digital Consumer Rights Commitments'. As indicated in the EU Commission website, the Product Safety Pledge sets up areas where online intermediaries and other actors voluntarily agree to take specific actions with respect to the safety of non-food consumer products sold online by third parties on their marketplaces. The aim is to

improve the detection of unsafe products marketed in the EU before they are sold to consumers or as soon thereafter as possible, and to improve consumer protection. The Digital Consumer Rights Commitments address some of the key aspects of consumer rights when using online marketplaces. They include commitments regarding the transparency of important information and marketing tools, namely consumer reviews and influencer marketing, as well as leverage the power of marketplaces to facilitate the exercise of certain EU consumer rights, and to offer training and advice to sellers operating on the marketplaces.

3. *The Protection of Consumer of Digital Goods*

The expansion and specification of the notion of 'consumer goods' in the online/digital context are primarily owed to Directive 770/2019 and Directive 771/2019, through the introduction of the new categories of 'digital content', 'digital services', and 'goods with digital elements'.

Beyond digital services («a service that allows the consumer to create, process, store or access data in digital form;» or «a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service»; Dir. 2019/770, art. 2, n. 2), a fundamental distinction is introduced between ‹digital content› and ‹goods with digital elements.›

'Digital content' refers to digital data, which is a res (a thing), although intangible and without physical substance, that (produced or supplied) in digital form satisfies a consumer's need (for instance, operating systems, applications and any other software, as mentioned by Whereas n. 14 of Dir. 2019/771).

'Goods with digital elements' remain traditional tangible movable goods (res corporee and tangible) but require the presence of or connection with digital content or a digital service for satisfactory consumer use. The category of 'goods with digital elements' includes any physically tangible item (movable material good) that has, among its essential elements for performing its functions (elements that must not be missing or compromised, as this would result in the loss of the good's functionality), digital content or a digital service. Thus, it is a movable good characterized by an additional feature represented by the digital content or service. The digital content or service can be an integral part of the good in question (incorporated within it) or, although external, must be interconnected

with the good in some way. Conversely, a material medium that solely serves as a carrier of digital content (such as a pen drive, whose only function is to store and transport data) is not considered a good with digital elements (Dir. 2019/771, art. 3).

In a nutshell, regarding the acquisition through specific contracts of digital content and digital services, by virtue of Directive 2019/770, the European consumer receives a new and specific uniform protection (according to the full targeted harmonization model, which allows Member States to introduce provisions aimed at ensuring greater protection of consumer interests than those provided for by the directive only when expressly provided for by the directive itself) with respect to the supply of digital content and services, the conformity with what is contractually provided for digital content and services, the remedies activable by the consumer himself in case of lack of said conformity and the consequences of possible modifications of digital content and services.

In relation to goods with digital elements, in turn, Directive 2019/771 extends, modernizes and specifies the already consolidated European discipline referred to in Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees, which for about twenty years has constituted a fundamental element of uniform European protection. Thanks to this directive, in fact, the European discipline on the conformity of goods to the contract, remedies in case of lack of conformity, methods of exercising such remedies and commercial guarantees, now finds a clear and specific application to goods with digital elements.

In any case, it is important to emphasize that with the new provisions contained in the two 2019 directives, the European multilevel legal system takes another significant step forward in the realization of the digital single market, increasing and specifying the protection of consumers with respect to digital consumer goods and services (and, therefore, hopefully, their trust in the purchase of digital content and services, as well as goods with digital elements), at the same time increasing the legal certainty of the context in which businesses operating in the European market operate (with a subsequent reduction in transaction costs).

4. *The Consumer's Personal Data as Consideration*

In defining the scope of application of Directive 2019/770, the European legislator appears to be addressing a general topic that has been

widely discussed and debated, in some way central to how consumers manage their personal data in relation to the 'consent or pay' business model (which involves a model that offers consumers-users the option to choose between giving their consent to the use of their personal data for advertising purposes or paying to use services or content without sharing such information), more recently developed by large social platforms (which, it is worth noting, have oriented themselves towards this model after the introduction of European data protection regulations).

In fact, the provision contained in Art. 3, par. 1, of Directive 2019/770 establishes that the consumer protection discipline applicable to contracts for the supply of digital content or services applies not only in cases where the consumer's counter-performance is represented by a price, i.e., in contracts that involve the payment of a sum of money, but it is explicitly provided that the consumer benefits from the protection discipline also in the event that the consumer, without paying anything, simply provides their personal data to the professional economic operator so that it can process them.

It has been asked whether, in this way, the European legislator has implicitly recognized the economic value of the personal data provided – more or less consciously – by the consumer, thereby appearing to be in apparent contradiction with Whereas n. 24 of Directive 2019/770, which states that personal data cannot be considered a commodity.

Regarding this, probably, by avoiding the main theoretical debate about the nature – commodity or non-commodity – of personal data (and thus about its marketability or lack thereof), the directive's provision should be read in relation to the limited but important goal of protecting consumers, namely to ensure that any digital content or service supplies that appear not to be backed by a consumer counter-performance could not be exempted from the mentioned uniform protection.

Regarding the 'consent or pay' business model, in particular developed by large online platforms, the European Data Protection Board (EDPB) has recently adopted an Opinion based on Article 64, paragraph 2, of the General Data Protection Regulation (GDPR) and the case law of the European Court of Justice in case C-252/21, *Bundeskartellamt*.

In particular, the EDPB considers that, in most cases, it will not be possible for online Platforms to comply with the requirements for valid consent provided by the GDPR, if they offer users only a binary choice between (a) consenting to processing of personal data for behavioural advertising purposes and (b) paying a fee.

The EDPB estimates that offering only a paid alternative to services

which involve the processing of personal data for behavioural advertising purposes should not be the default way offered by controllers (i.e., the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data). When developing alternatives, online platforms should consider providing individuals with an 'equivalent alternative' that does not entail the payment of a fee. EDPB points out that any fee charged cannot make individuals feel compelled to consent. Controllers should assess, on a case-by-case basis, both whether a fee is appropriate at all and what amount is appropriate in the given circumstances. Large online platforms should also consider whether the decision not to consent may lead the individual to suffer negative consequences, such as exclusion from a prominent service, lack of access to professional networks, or risk of losing content or connections. The EDPB notes that negative consequences are likely to occur when large online platforms use a 'consent or pay' model to obtain consent for the processing.

5. *Social Platforms Services and User-Consumer Protection*

Among the most appreciated digital services by consumers are undoubtedly the services (apparently free, as long as one does not consider the personal data that social platforms collect in exchange for access to their services) offered by social platforms, namely those online computer services that enable the creation of virtual social networks by allowing users to share textual content, images, videos, and audio and interact with each other, and whose daily use makes our life experience increasingly hybrid between real places and activities and virtual places and activities, so much so that it has been evocatively rebranded 'onlife'.

It is undeniable that Social Platforms are today economic entities with a powerful de facto power, largely dominating the digital world, both with respect to other businesses engaged in economic activity in the digital context (through them or in competition with them) and with respect to the multitude of physical individuals who (for non-professional needs) use Social Platforms (and at the same time making the existence of Social Platforms more successful). Social Platforms have now become an element so important in the daily life of the vast majority of people – not just a recreational or entertainment opportunity, but also a virtual space for projecting one's identity, weaving personal relationships, expressing

and communicating one's thoughts – that these individuals cannot give them up.

Regarding the importance to their life and the pervasiveness of Social Platforms, the user-consumer is subject to at least a triple order of themes with legal relevance:

a) Social Platforms offer people their services according to a 'take it or leave it' business model, with unilateral predisposition of the terms and conditions of access and use of the platform, without any possibility of negotiation and modification of these terms and conditions, as well as with a tendency towards absence of contractual obligations binding on them;
b) user-consumers find themselves acting in a para-legal system that proposes itself as autonomous to some extent from the state legal system (or, at least, that aims to make recourse to state-administered justice superfluous); this 'private' system recognizes rights, identifies prohibitions and regulates the responsibility of users according to what is established by the Social Platform, with the application of its own sanctioning apparatus, more or less preceded by forms of confrontation with users; the 'grip' of the Social Platform on this para-legal system (and its aspiration of autonomy and self-completeness) manifests itself in all its breadth and strength when the Social Platform decides to exclude from the service offered the person who, in its unquestionable judgment, has violated the standards that the Social Platform itself dictates to all its users;
c) in relation to the provision of their online service to people, Social Platforms move within a regulatory system that tends to establish their irresponsibility, even of an extra-contractual nature, with respect to what is unlawful to the detriment of their user-consumers (or other people) that occurs through the service they offer.

Regarding the first topic, it is to be considered that even the user of the services offered by the Social Platform benefits from the protection ensured by European harmonization laws (and the subsequent national implementing regulations) for consumers when they establish contractual relationships with professional economic operators. Specifically, this concerns laws on the following matters:

a) pre-contractual information, formal requirements and right of withdrawal in off-premises and distance contracts (aspects recently updated by Directive 2011/83/EU);
b) prohibition of unfair contract terms and clauses (matter regulated

by Directive 93/13/EEC, whose sanctioning aspects have been specified and made more effective by Directive (EU) 2019/2161);

c) prohibition of unfair commercial practices (Directive 2005/29/EC, whose sanctioning aspects have been specified and made more effective by Directive (EU) 2019/2161).

Therefore, without being able to examine these provisions in detail here, even the online consumer, who becomes a contractual counterparty to the Social Platform, can theoretically resort to the remedies prepared by individual national legislators in the event of abusive clauses or conditions, deceptive or aggressive commercial practices, or lack of contractual information attributable to the Social Platform.

However, it must be considered that even the online consumer suffers from an objective (in the sense that it is objectively impossible for a consumer to negotiate the contractual terms of their legal relationship with the Social Platform in advance) and subjective (in the sense that almost no consumer is interested in knowing in advance the legal terms of their relationship with the Social Platform, eager as they are to access the apparently free services offered by the Social Platform) inability to influence the terms and conditions of their contractual relationship with the Social Platform.

This situation of apparent unchangeability of the legal terms of the relationship imposed by the Social Platform on the consumer is then exacerbated by the circumstance that – and I pass here to consider the second profile mentioned above (the creation by Social Platforms of autonomous and 'closed' para-legal systems) – Social Platforms seek to maintain a stronger possible control over conflicts and disputes (i) between their own users-consumers and (ii) between these and the Social Platform itself, playing both the roles of 'legislator' and 'judge' of the digital world (even if it appears to be without physical territory) composed by the 'people' of the Social Platform users and the digital activities that take place on it or through it.

The legislative role of the Social Platform community is exercised by these platforms through the so-called Community Standards. These Standards are determined autonomously by the Social Platforms and represent the principles and values in which (upon request by the Social Platform, which allows access to its services only after the user accepts these standards) the entire community of users who access the Social Platform must recognize and behave accordingly. In the absence of compliance with the Community Standards, the Social Platforms have on several occasions removed published content that they deemed did not respect the Standards and even excluded (temporarily or definitively) the

user who published it from accessing the Social Platform and its services, thus becoming the judge of the respect of their own Standards.

This conduct of the Social Platforms has led to the activation of various disputes with their own user-consumers, which arise from a different evaluation, by the Social Platform and the user-consumer, of what the user himself published on the platform and what the platform evaluates be respectful of the Community Standards, with a factual limitation by the Social Platforms of the freedom of thought of individuals, which, it is remembered, is a constitutionally guaranteed right in almost all legal systems.

Regarding this, it should be noted that the Community Standards (as mentioned, established autonomously by the Social Platform and configuring the set of ethical, political, and social values that the platform admits and promotes in the relationships between all its users) have a scope of application that claims to be global, extraterritorial with respect to the national legal systems in which the Earth is still divided today. This follows from the circumstance that the virtual world of the platform has no physical territory and can be accessed from various places on Earth, without accounting to any state powers. The Social Platforms thus have an innate tendency to create 'places' devoid of any application of state law, in which the *Grundnorm* can be represented precisely by the Community Standards, the respect of which is ensured by the Social Platform itself and its unequivocal power to moderate and remove user content, applying, as an extreme sanction, the suspension of access (even definitively) to the platform.

As mentioned, the Social Platform proposes itself as the custodian of the Community Standards and judge of their respect, also offering para-jurisdictional systems for resolving disputes between the Social Platform and its own user-consumers.

The most evolved, studied, and epigrammatic example of these para-jurisdictional systems is undoubtedly represented by the Facebook Oversight Board (*https://www.oversightboard.com*), whose decisions are considered binding by Facebook and Instagram. Regarding this phenomenon, high has been the concern of constitutional and public law scholars who have drawn attention to the risks connected to the possible evaporation of state constitutional rights and the overcoming of the delicate balances entrusted to democratic Constitutions, the privatization of digital justice on a global scale, and this further possible manifestation of the crisis of state sovereignty and erosion of the state monopoly on jurisdiction.

On the other hand, it should not be forgotten that this will of the Social Platform to be itself the legislator and judge of the Community Standards and, in a broader sense, of human activities (or not) that take

place on and through the Social Platform, in some cases clashes with the persistent will of users to contest the choices of the Social Platform by turning to state judicial authorities, usually of the state where the user resides (perhaps being a citizen) and which the user instinctively feels as an institution capable of ensuring justice in the confrontation with the Social Platform. In these cases, the conduct of the Social Platform in applying the extraterritorial Community Standards is evaluated based on the law of a national state and/or international treaty law to which that state adheres. About these hypotheses, it should be observed that in the face of the claimed transnationality of the Community Standards, the still existing territoriality of individual national legal systems and their coercive jurisdictional power prevail (while a system of real protection of online service user-consumers worldwide is completely lacking).

Finally, regarding the profiles of responsibility borne by Social Platforms for any potential illegal acts committed by their own user-consumers against other user-consumers (or even non-user-consumers), these platforms enjoy in the European context a tendency towards irresponsibility, which however appears to be currently under review.

At the beginning of this century, the so-called E-commerce Directive (Dir. (UE) 2000/31) formalized the principle (Art. 14 of the E-commerce Directive) that the hosting provider (i.e., the one responsible for storing the information provided by a user) would be exempt from liability as long as it was not actually aware of the illegality of the information or not aware of facts or circumstances that made the illegality of the information manifest; on the other hand, as soon as it became aware of these facts, the hosting provider was required to immediately remove the content. Art. 15 of the E-commerce Directive specified in addition that there was no general obligation of surveillance or search on the part of the Social Platform for illegal activities. In this period, the Court of Justice of the European Union progressively identified the categories of passive hosting provider (which was considered to be able to continue to benefit from the so-called 'safe harbor' i.e., the exemption from liability, as it did not know, nor controlled the stored information; ECJ, September 15, 2016, *McFadden*, C-484/14, § 62) and active hosting provider (ECJ, September 11, 2014, *Papasavvas*, C-291/13, ECJ, *Google France*, C – 236/08, ECJ, *L'Oréal*, C-324/09, § 123, ECJ, August 7, 2018, *Coöperative Vereniging SNB-REACt U.A. c. Deepak Mehta*, C-521/17), which was considered not worthy of benefiting from the safe harbor, as it performed an additional activity beyond the simple and neutral storage of information, somehow actively interfering with the publication of the content by the user (which

was identified based on the presence of one or more of the so-called 'indices of interference', such as, for example, an activity of filtering, selection, indexing, organization, cataloging, aggregation, evaluation, use, modification, extraction, or promotion).

Today, although art. 12 to 15 of the E-commerce Directive have been repealed, the provisions contained in Chapter II of the DSA remain in line with the general approach already acquired with the E-commerce Directive, introducing a series of graded procedural and substantive obligations. These obligations strengthen the principle of accountability of Social Platforms (as well as all Internet Service Providers) and mark the transition from mere liability (in certain conditions) to responsibility with respect to specific duties of diligence (which are substantiated by the execution of a series of risk assessments and prevention and containment activities of risks inherent in the digital environment) in the performance of their business activity.

Firstly, the DSA confirms the framework of the E-commerce Directive and, on the one hand, reiterates (Art. 8) that there is no general obligation to monitor stored or transmitted information, nor to verify the facts indicating the presence of illegal activities; on the other hand, it renews (Art. 6) the rule according to which the Social Platform is not responsible for stored (and transmitted) information on the user's request, provided that a) it is not actually aware of illegal activities or contents and, in the context of claims for damages, is not aware of facts or circumstances that make the illegality of the activity or contents manifest; or b) it becomes aware of such illegal activities or contents or becomes aware of such facts or circumstances, it acts immediately to remove the illegal contents or disable access to them.

On another level, the DSA imposes on Social Platforms to inform without undue delay the authority (judicial or administrative) that has issued an order to counteract one or more specific illegal contents of having followed that order (Art. 9), as well as, having received an order to provide specific information on one or more individual service recipients, to inform without undue delay the authority (judicial or administrative) that issued the order of the receipt of the same and the follow-up they gave it (Art. 10).

As mentioned, the true step forward taken by the DSA lies in the introduction of a series of obligations that detail the duty of diligence (also) of Social Platforms, distinguishing between Social Platforms and very large Social Platforms, for the latter meaning those platforms whose average monthly active service recipients in the Union are equal to or greater than 45 million and which the Commission has designated as

such (with a decision of April 25, 2023, the European Commission has designated 17 Very Large Online Platforms, or VLOPs, based on the data published as of February 17, 2023).

Beyond a series of diligence obligations for a transparent and safe online environment applicable to all intermediate service providers (Social Platforms included), the DSA establishes more rigorous standards of transparency and responsibility for Social Platforms regarding content moderation, advertising, and processes based on the use of algorithms, and also imposes obligations for risk assessment and development of risk management systems.

In particular, the DSA provides for (i) a first series of additional obligations (Articles 16 to 18) applicable to hosting providers and, therefore, also to Social Platforms, (ii) a second series of additional obligations intended only for Social Platforms (Articles 19 to 32) and (iii) a third series of additional obligations (Articles 33 to 43) borne only by Very Large Online Platforms (VLOPs).

6. *Online Markets and Consumer Protection*

The increasing recourse by consumers to online purchases on so-called 'online markets' has made it necessary for the European legislator to intervene to specify the protection of consumer rights and interests in the new market context and with respect to new possible unfair commercial practices.

The Directive (EU) 2019/2161 regarding the better enforcement and modernization of Union consumer protection rules (the so called 'Omnibus Directive') has thus introduced into the Directive 2005/29/EC on unfair commercial practices the definition of 'online market'. An online market is a service (offered by a professional economic operator) that uses software that allows consumers to conclude distance contracts (not necessarily at a cost) with professional economic operators or other consumers. The professional economic operator who offers the online market service can be the same professional economic operator who sells (through the online market) the product to the consumer or a different professional economic operator (who manages only the online market service and is not the seller of the product).

Under the aspect of consumer protection with respect to unfair commercial practices (and particularly of a misleading omission of relevant information) in relation to products offered on online markets,

it must now be specified whether the one (who is not the manager/provider of the online market) who formulates a purchase invitation is a professional economic operator or a third party.

The Omnibus Directive (Art. 6 bis) has also introduced a series of specific information obligations for the online market provider in relation to contracts concluded on online markets.

The online market provider (i.e., the one who makes available the online market tool to conclude B2C or C2C contracts) must communicate to the consumer who accesses the online market to conclude contracts through it a series of specific information in a clear and understandable manner and in a way appropriate to the means of distant communication. These specific information must be provided to the consumer before the moment when the consumer can be bound by a distance contract or before a binding offer is made.

In particular, the online market provider must: (i) make available to the consumer, in a dedicated section of the online interface (such section being directly and easily accessible from the page where the offers are presented to the consumer), general information about the main parameters that determine the classification of the offers presented to the consumer as a result of their search, as well as information about the relative importance of these main parameters compared to other parameters; (ii) clarify whether the third party offering goods, services, or digital content on the online market is a professional economic operator or a subject to whom such status is not attributed; this clarification will be provided based on the declarations made by the aforementioned third party to the online market provider; (iii) if the third party offering goods, services, or digital content is not a professional economic operator, inform consumers accessing the online market that contracts concluded on the online market with such non-professional economic operator do not apply the consumer rights derived from European Union law on consumer protection; (iv) if the contract concluded or to be concluded through the online market provides for the allocation of obligations arising from the contract between the online market provider and the third party offering goods, services, or digital content, provide the consumer with information about the manner of such allocation; the communication of such information leaves unaffected the responsibility that the online market provider or the professional economic operator concluding the contract through the online market may have in relation to the contract under other European or national laws.

Anyway, the provisions on information obligations provided by other European regulations continue to be applicable to online market providers.

7. *The Circulation of Consumer's Personal Data*

As mentioned, the digital consumer is the main provider of personal data (and non-personal data) that enables the data economy underlying the commercial and economic power of most modern technology companies.

As a physical person, the digital consumer benefits first and foremost from the protection ensured by the GDPR regarding the processing of their personal data. This is a comprehensive, articulated protection that must necessarily interact – as recognized by the GDPR itself – with the free circulation of such data within the Digital Single Market and beyond.

A complete analysis of how the GDPR protects the rights of the digital consumer regarding their personal data is not possible here, but it is interesting to briefly address the topic of protecting the personal data of European digital consumers outside of the European territory. Specifically, I refer here to the debated issue of transferring the personal data of European digital consumers to the United States, which has led to various judgments by the Court of Justice and various agreements between the European Union and the United States.

The regulatory framework is currently contained in Chapter V of the GDPR titled «Transfer of personal data to third countries and international organizations» (Articles 44 et seq.).

The general principal for transfers is the following: «Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined» (art. 44).

In compliance with the above mentioned principle, the transfer of personal data to third countries can generally occur (i.e., without specific authorizations) only if the European Commission has decided – with an 'adequacy decision' – that the third country ensures an adequate level of data protection (Article 45).

Under the Directive 95/46, with an adequacy decision (Decision 2000/520, known as 'Safe Harbor'), the Commission had declared that the transfer of personal data to the United States was assisted by an

adequate level of protection when it occurred in accordance with the so-called 'Safe Harbor Privacy Principles' established by the same decision and additional guidelines.

However, in 2015 (with the judgment in Case C-362/14, known as 'Schrems I', named after the Austrian activist who initiated the national procedure), the Court of Justice annulled the Commission's adequacy decision, considering that the United States could not be considered a third country with adequate levels of protection for personal data and fundamental rights, especially due to the possibility for American authorities to access the information of European citizens without sufficient safeguards for these individuals.

To enable a legitimate general transfer of personal data of European citizens to the United States (clearly of interest to major American technology companies), the European Commission has, therefore, approved a new adequacy decision (known as 'Privacy Shield') to take into account what the European judges had stated. However, even this adequacy decision fell under the axe of the Court of Justice (Case C-311/81, known as 'Schrems II') in 2020, still due to the lack of adequate guarantees, including the presence of acts and executive orders in the American legal system that were so invasive that they would not have ensured a level of protection substantially equivalent to the GDPR.

Following Schrems II, between the European Commission and the United States, an agreement called 'Trans-Atlantic Data Privacy Framework' was reached in 2022 with the aim of introducing a new regulatory framework for the legitimate transfer of personal data of European citizens from the EU to the United States. After the signature by US President Joe Biden (Enhancing Safeguards for United States Signals Intelligence Activities), which aims to strengthen the protection of privacy and civil liberties applicable to US intelligence activities, the European Commission took another adequacy decision in July 2023 (C(2023) 4745 final).

Even with regard to the new Data Privacy Framework and the subsequent adequacy decision, some concerns have been raised about the substantial equivalence between the US discipline and the requirements demanded by European law. Therefore the issue does not appear to be resolved in a stable manner.

8. *Online Searches and Reviews*

The centrality of digital communication tools for consumers results in the fact that today the consumer performs online many activities that were previously carried out through other (analog and non-digital) means. Now, almost all product searches by consumers are performed online (at least in an initial phase, of first orientation to purchase) and consumers are increasingly inclined to share online their evaluations of products and services (not necessarily digital) they have purchased or used (even without an online purchase or delivery).

The Omnibus Directive (Article 3, which modified Article 7 of Directive 2005/29) has established what information must be provided to the consumer when they proceed through an online interface to conduct a search for possible products of their interest regarding a specific need they may have, possibly offered by professionals or consumers and, in some way, advertised online. As is known, such searches lead to an exposure, in the form of a ranking, of products that the search (carried out based on algorithmic parameters establishing scales of values) considers of interest to the consumer who performed the search based on the generic criteria set by the consumer themselves.

The consumer must be provided with general information about the main parameters that determine the classification of the products presented to the consumer as results of the search and the relative importance (i.e., the relevance in determining the classification) of the individual parameters considered compared to other parameters.

The aforementioned general information on the main parameters used to conduct the online search must be provided independently of the location where the operations (presumably of purchasing the products) will be actually concluded (i.e., also outside and without using online markets). The information must be provided in a dedicated section of the online interface visible and accessible to the consumer. This section must be directly and easily accessible for the consumer from the online page where the search results are presented (presumably through a link easily identifiable by the consumer).

The protection of the consumer with respect to online searches is completed by the provision that any commercial practice consisting of the omission of clear indication, within the exposure of the results of an online search performed by a consumer, that one of the results is a paid advertisement or that a specific classification of a product in the

hierarchical display (to be understood in a broad sense, both as pure ranking and as better or highlighted visualization on the web page) of products contained in the search was determined by a specific payment preordained for that purpose (Omnibus Directive, Art. 3, which modified Annex 1 of Directive 2005/29/EC).

Within the scope of possible omissions, the Omnibus Directive (Art. 3, which modified Art. 7 of Directive 2005/29/EC) has introduced some information obligations regarding the reviews compiled and provided by consumers and which the professional economic operator has collected and decided to make public. The provision clearly refers to the practice now widespread among many professionals of promoting their products by inserting on their commercialization website the reviews (usually only the positive ones) that consumers have given regarding the products.

Regarding the content of the information obligations related to the reviews published for the purpose of configuring a possible omission, the norm indicates that the professional economic operator must inform consumers accessing the reviews whether these reviews come from other consumers who have actually purchased or used the product and how he is able to ensure this circumstance. With respect to this probative aspect, it can be reasonably considered that this obligation is fulfilled if the professional economic operator puts the consumer in a position to verify – upon request by the consumer – the origin of the review and its main data.

9. *Portability and Geoblocking*

The digital consumers are modern consumers who tends to move, often, outside their national and territorial market. When they move physically outside their own country, the digital consumers consider it important to be able to continue to enjoy the digital services and content they used in their national market, and even when they do not move physically and intend to acquire goods and services offered by professional economic operators located in other Member States, they suffer from being subjected to practices that preclude cross-border markets.

Within the framework of the realization of the digital single market, the European legislator has appropriately intended to take charge of these important issues for the digital consumer and consumers in general.

With reference to the first aspect, in June 2017, Regulation (EU)

2017/1128 was adopted (applicable from April 2018). This Regulation introduced the right of EU citizens (who are temporarily in another Member State) to access paid-for online content services in other EU Member States, in the same way as they would in their home country, as part of the EU digital single market. In particular, such guarantees that the content available in other Member States should be: the same content; on the same range and number of devices; for the same number of users; with the same functionality; and with no extra charges. There is no obligation to provide similar quality unless this is agreed on with the subscriber, but the quality must not be deliberately reduced, and the subscriber must be informed about the quality of delivery before the service is provided.

With regard to the second aspect, in February 2018, the European legislator adopted Regulation (EU) 2018/302 (the so called 'Geo-blocking Regulation' applicable since December 2018), which, in summary, prohibits unjustified discrimination of consumers (but also undertakings purchasing as end users) shopping online, purely based on their nationality, place of residence or place of establishment. This prohibition of discrimination includes situations where a customer buying across borders is prevented from finalising the purchase, or is asked to pay with a debit or credit card from a certain country. The goal of the Regulation is to increase opportunities for consumers and businesses to buy across borders.

In November 2020, the Commission published the first evaluation of the impact of the Geo-blocking Regulation and analyzed the possibility of extending its application to specific digital services offering copyright-protected content (such as e-books, music, software and online games), as well as to audiovisual services. Dissatisfied with the current situation and implementation of the Regulation (EU) 2018/302, in December 2023, the European Parliament adopted a resolution in which the need to revise European rules on geo-blocking in light of the acceleration of digital transformation and the increase in online purchases in recent years was underlined. The issue appears to be particularly felt with reference to audiovisual services, still stubbornly offered to consumers in relation to well-compartmentalized national markets.

10. *Electronic Communications and Consumer Protection*

The Directive (EU) 2018/1972, which establishes an European Code of Electronic Communications (replacing Directives 2002/19/CE, 2002/20/CE, and 2002/21/CE), contains an updated set of provisions to regulate electronic communications (telecommunications), telecommunications services, and associated structures and services. This has also led to an increase in the level of consumer protection.

Under this latter aspect, the articulated European directive contains: (i) provisions aimed at making it easier for consumers to switch between service providers and offering better protection; (ii) a mechanism to ensure that consumer rights remain intact and updated when changes occur in business models and consumer behavior; (iii) provisions aimed at guarantying access to adequate and affordable high-speed internet for all consumers, regardless of their location or income.

11. *Product Liability and AI Liability*

If a consumer encounters defective products that have caused harm (even death), they are protected by one of the earliest consumer directives: Council Directive 85/374/EEC regarding liability for damage caused by defective products.

To better consider changes generated by digitalization of products, the European Commission proposed to modify the 1985 directive in September 2022 (COM(2022) 495 final) by expanding the definition of a product to include software updates, artificial intelligence, and digital services. The proposal also specifically considered the compensation for psychological damages (requiring therapy or medical treatment) and the destruction or irreparable damage to data, extending the period of responsibility to 30 years, along with other improvements in the interest of consumers. The proposal was recently adopted through Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

However, the most significant change in the coming years will likely be the introduction of uniform European rules that, by integrating the review of the 1985 directive, will better address harm caused by illegal

actions of artificial intelligence systems or those committed through such systems.

Regarding this profile, the European Commission presented a proposal in September 2022 (COM(2022) 496 final) for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

The new rules intend to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies in the EU. The AI liability directive would create a rebuttable 'presumption of causality', to ease the burden of proof for victims to establish damage caused by an AI system. It would furthermore give national courts the power to order disclosure of evidence about high-risk AI systems suspected of having caused damage. Stakeholders and academics are questioning, inter alia, the adequacy and effectiveness of the proposed liability regime, its coherence with the AI Act jut adopted, its potential detrimental impact on innovation, and the interplay between EU and national rules.

12. *Table of Legislation, Official Documents, Case Law*

Legislation

- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
- Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
- 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 (Unfair Commercial Practices Directive)
- 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
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market
- Directive (EU) 2018/1972 of the European parliament and of the Council of 11 December 2018 establishing the European Communications Code
- 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 Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services
- Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC
- Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services
- 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, 2005/29/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
- 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 (Digital Services Act)
- Proposal COM(2021) 206 final for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts
- Proposal COM/2022/496 final for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828
- Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

Official Documents
- Communication of April 2018 significantly titled 'A New Deal for Consumers' (Communication from the Commission to the European Parliament, the Council and the Economic and Social Committee of April 11, 2018, COM(2018) 183 final
- 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce
- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield
- Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework

Case Law

- ECJ, March 23, 2010, *Google France*, C–236/08
- ECJ, July 12, 2011, *L'Oréal*, C-324/09
- ECJ, September 11, 2014, *Papasavvas*, C-291/13
- ECJ, October 6, 2015, *Schrems I*, C-362/14
- ECJ, September 15, 2016, *McFadden*, C-484/14
- ECJ, August 7, 2018, *Coöperative Vereniging SNB-REACt U.A. c. Deepak Mehta*, C-521/17
- ECJ, July 16, 2020, *Schrems II,* C-311/18
- ECJ, July 4, 2023, C-252/21, *Bundeskartellamt*.

13. *Readings*

Buratti A., *Framing the Facebook Oversight Board: Rough Justice in the Wild Web*, Medialaws, 2/2022, p. 31-48

De Gregorio G., Goanta C., *The Influencer Republic: Monetizing Political Speech on Social Media*, German Law Journal, vol. 23, 2022, p. 204-225

De Vries S., Kanevskaia O., de Jager R., *Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation*, European papers, vol. 8, 2023, p. 583-610

Duivenvoorde B., *Consumer Protection in the Age of Personalised Marketing: Is EU Law Future-proof?*, European papers, vol. 8, 2023, p. 631-646

D'Amico A.S., *Market Power and the GDPR: Can Consent Given to Dominat Companies Ever Be Freely Given?*, European papers, vol. 8, 2023, p. 611-629

Floridi L. (ed.), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, 2013

Frosio G., Geiger C., *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, European Law Journal, vol. 29, 2023, p. 31-77

Sander B., *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, Fordham Int'l Law Journal, vol. 43, 2020, p. 939-1006

Stiković S.K., *The EU' Digital Services Act and Its Impact on Online Platforms*, European Union law Working Papers, n. 85, 2024

Zardiashvili A., Sears A.M., *Targeted Advertising and Consumer Protection Law in the EU*, Vanderbilt Journal of Transnational Law, vol. 56, 2023, p. 799-852

Zeno-Zencovich V., *The EU regulation of speech. A critical view*, MediaLaws, 1/2023, p. 11-18