Public Governance, Administration and Finances Law Review Vol. 9. No. 1. (2024) • 37–58.

DOI: 10.53116/pgaflr.7134

Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act[I]

Domingos Soares Farinho*

* Assistant Professor, Faculty of Law, University of Lisbon, Lisbon, Portugal, e-mail: domingosfarinho@fd.ulisboa.pt

Submitted: 13 December, 2023 | Accepted: 2 May, 2024 | Published online: 27 June, 2024

Abstract: The new EU Digital Services Act (DSA) is intended to regulate intermediary service providers, with particular attention to online platforms and search engines. The core activity of such platforms and engines is personal data processing, pursuant to the tasks of content moderation and recommendations. This means that regarding personal data, there is an interconnection between the GDPR and the DSA, and it is a matter of law to determine how they interact in the EU digital space. This paper endeavours to draw a comprehensive picture of how the GDPR and the DSA seek to provide better guidance on the adequacy and enforcement of personal data protection. It is argued that their relationship is best described as the DSA being the *lex specialis* vis-à-vis the GDPR, but this is somewhat blurred by instances where the latter is mostly complementing the former, such as 1. specific legal basis for data processing in compliance with new legal obligations for platforms; 2. a new articulation between both regulations concerning dark patterns; 3. new prohibitions on personal data processing; 4. new duties for the protection of personal data; and 5. a new ancillary institutional framework to regulate data protection by online platforms in collaboration with national data protection authorities.

Keywords: Digital Services Act, GDPR, data protection, personal data, content moderation, profiling

[I] This paper was first presented at the Forum on Privacy and Governmental Transparency (Ludovika University of Public Service) on 8 June 2023.

1. Introduction

Online platforms and online search engines[1] have become some of the most significant processors of personal data in the world (Dijck et al., 2018, p. 13; Taddeo & Floridi, 2017a, p. 1; Taddeo & Floridi, 2017b, p. 13; Kurtz et al., 2019, pp. 5059–5068; Kurtz et al., 2022) due to their growing importance in the digital economy and in our daily lives (see Turillazzi et al., 2023, p. 6). From a legal perspective, this phenomenon raises the question of how users' personal data can be protected without disproportionally encroaching upon the freedoms of online platforms and other users. Legal systems address this issue in different ways but in the EU, the Digital Services Act (DSA) is intended to ensure a fundamental rights-based approach to regulating online platforms (Recital 3), meaning that the protection of personal data plays a central role.

The DSA is part of the European Union's Digital Strategy[2] which encompasses wide-ranging legislation including the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Artificial Intelligence Regulation (AI Act), and the European Chips Act. The DSA aims to play a key regulatory function within the EU Digital Strategy; its purpose is to regulate information society "intermediary services"[3] with a special focus on "online platforms". The DSA builds upon the e-Commerce Directive of 2000,[4] in which the concept of "intermediary service" was already central, but the act has further refined these categories. In the Directive, there was a simple threefold distinction made between "service providers" consisting of 1. providers of mere conduit services, 2. providers of caching services and 3. providers of hosting services. While retaining this threefold distinction (with "service providers" now referred to as "intermediary services"), the DSA differentiates between two new sub-categories within hosting services – "online platform" and "online search engine" – and one additional sub-category within each: "very large online platforms" (VLOP) and "very large online search engines" (VLOSE)[5]. Each new category is subject to additional rules, leading to stricter regulations being applied at the top of the pyramid (see Figure 1 below).

Thus, online platforms and online search engines refer to specific categories within the broad range of information society intermediary services covered by the subject matter of the DSA [see Article 2(1)]. Specific Sections of the DSA[6] have been dedicated to legally defining online platforms, simply because the business model of such platforms (as defined by the DSA) makes them fully dependent on personal data as "user-generated content

[1] This paper uses the definitions of "online platform" and "online search engine" in accordance with Article 3(j) and 3(i) of the Digital Services Act, 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 (hereinafter, the DSA).

[2] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015) 192 final (Digital Single Market Strategy); see also: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en.

[3] See Article 3(g) DSA.

[4] 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).

[5] See Article 33 DSA.

[6] See Sections 3 through 5 of Chapter III of the DSA.

(UGC)" (York & Zuckerman, 2019, p. 138; Hartmann, 2020). These platforms collect personal data and process and monetise it in exchange for a service: allowing personal data subjects, i.e. users, to share their content online. Thus, personal data, within the business model of online platforms and search engines can be seen as a specific type of content *submitted to* and *provided by* those platforms and engines, at least in most cases. This point is important for understanding that although in the field of online platforms, both from a legal and business perspective, *content* is the term preferred in most cases to describe and explain how these specific types of hosting services work, most of this *content,* being user-generated, should also be described as *personal data, submitted to* and *used by* online platforms and *made available* to a variable number of users. It should be added that the term "user" is being used here in the broad sense of Article 3(b), (p) and (q) of the DSA, which includes not only "users" in the sense of "registered users" who have undergone the account registration process, but also "users" as recipients of the service for the purpose of "being exposed to information" hosted and presented by the platforms and search engines.

Furthermore, as online search engines are treated in the same way legally speaking as online platforms,[7] all references to online platforms hereafter include online search engines, unless stated otherwise.

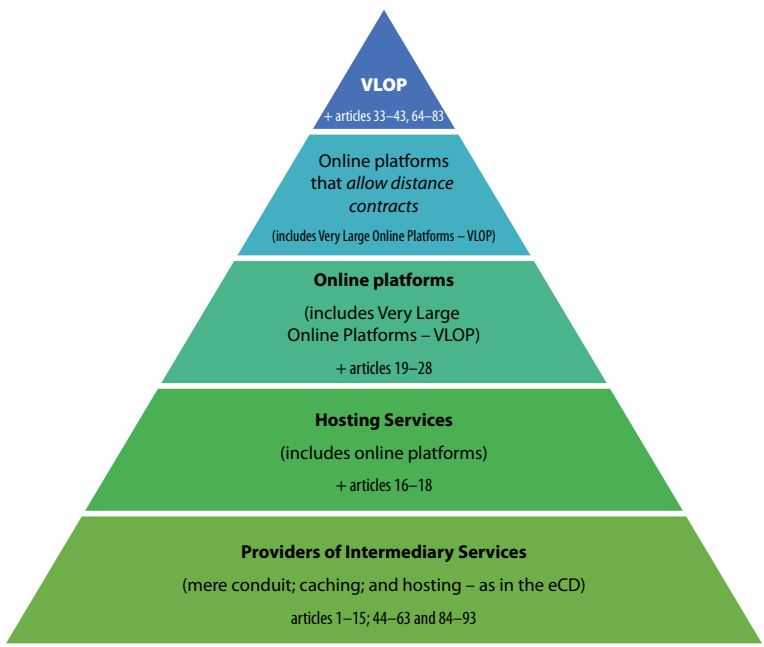

Figure 1.
The DSA regulatory pyramid

Source: Compiled by the author.

[7] In the original proposal for the DSA, the Commission did not differentiate between online platforms and online search engines; this distinction was introduced at a later stage.

The DSA has to be applied with reference to the two principal EU laws on personal data protection within the digital domain, i.e. the GDPR and the e-Privacy Directive.[8] This means that the processing of personal data by online platforms is an activity which is closely regulated by EU law. Due to the close interconnection of the latter three pieces of legislation, it is only possible to determine what this legislation covers after careful analysis of the framework in place.

This paper endeavours to address this question by focusing on the specificities of the regulation of personal data processing by online platforms in the EU. In Section 2, we will review how the GDPR applies to online platforms, given that they qualify as personal data controllers under the Regulation. This will allow us (in Section 3) to better determine and analyse the specificities introduced by the DSA for cases where personal data are processed by online platforms. Thus in Section 3.1, we first examine the general data protection framework under the DSA, by way of its two defining topics: the legal basis for processing personal data introduced by the DSA and the implications in terms of liability when data is being processed by online platforms. In Section 3.2, we progress to considering specific issues raised by the DSA concerning personal data protection on online platforms. We first examine the obligation to protect personal data, especially with respect to content moderation as online platforms' core activity, and then progress to automated processing of personal data. In Section 3.3, we examine online interface design and organisation prohibitions, in order to understand how the DSA adds a further layer of protection over and above that of the GDPR. In Section 3.4, we analyse prohibitions on profiling in relation to advertising, minors and recommender systems. In Section 3.5, there is an examination of the institutional regulatory dimension of the DSA as a personal data protection law. Finally in Section 4, we comment on the way in which the DSA addresses protection of online platform users' personal data. The position presented here is that the DSA operates as *lex specialis* in the field of personal data protection with respect to online platforms. It not only introduces 1. specific legal basis for data processing in line with platforms' new legal obligations, but it also introduces 2. new prohibitions on the processing of personal data, 3. new data protection obligations, and 4. a new ancillary institutional framework to regulate data protection by online platforms in collaboration with national data protection authorities.

2. Applying the GDPR to online platforms

Under the GDPR, online platforms are just another type of controller [see Article 4(7)], i.e. they "alone or jointly with others, determine the purposes and means of the processing of personal data". This means that they fall under the material scope of the

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

GDPR [Article 2(1)] and are required to provide lawful grounds for processing personal data [Article 6(1)].[9]

Personal data processing by online platforms occurs independently of any data subjects deciding to become *registered* platform users: online platforms also collect personal data from those data subjects who merely access the content shared on platforms, without registering for an account, and who, therefore, have no contractual relationship with the service.[10]

With respect to their users, online platforms are obliged to choose the applicable legal grounds for processing their personal data from the list set out by the EU legislator in Article 6(1) GDPR. An examination of this list reveals that, *a priori,* the legal basis foreseen by the legislator can be applicable to online platforms, depending on the circumstances and the services provided to users.[11] In case of online search engines, this appears to be more complex: depending on the specific service provided, it can be very difficult to accept the application of point (e) (reasons of public interest). The most common legal basis for online platforms to process personal data is either that such data is required in order to perform the contract between the user and the platform [Article 6(1)(b) GDPR], or the basis of user consent [Article 6(1)(a) GDPR]. In some instances, a platform's legitimate interests provide the basis for processing personal data [Article 6(1 (f)]. Nevertheless, it should be noted that given the legal definition of DSA for "online platform" and "online search engine", the personal data required to perform contracts for such services is very limited, especially in contrast to the quantity and uses of personal data required for their business model. As we shall see below, the DSA foresees some cases where it is necessary to process personal data in order to comply with the Act itself, thus falling under Article 6(1)(c).

No matter which grounds online platforms are relying upon, such grounds are subject to the principle of purpose limitation [Article 5(1)(a) GDPR]. Each of the grounds set forth under Article 6(1) is specifically linked to the principle of purpose limitation, inasmuch as the purpose for which personal data are processed is limited by the scope of the legal basis provided by the legislator. Consent [Article 6(1)(a)] depends on the purpose presented to the data subject; the scope of performance of a contract [Article 6(1)(b)] determines a purpose for the processing of personal data; legal obligations [Article 6(1)(c)] entail specific purposes and not others; the vital interests of users [Article 6(1)(d)] determine the precise purposes for which personal data are processed; the pursuit of certain public interests [Article 6(1)(e)] determines the purpose of personal data processing; and legitimate interests [Article 6(1)(f)] lead to different balancing outcomes depending on the purpose chosen.

Above and beyond the lawful grounds laid down in the GDPR, online platforms are always required to rely on consent in order to process personal traffic data for the "purpose of marketing electronic communications services or for the provision of value-added

[9] Online platforms and search engines may also be qualified as processors, but this would have to be ascertained for each specific case; see Article 4(8) GDPR.

[10] See, for instance, Facebook Privacy Policy, version of 2023.12.12.

[11] For instance, Meta considers that it may process personal data based on any of the lawful grounds foreseen under Article 6(1) of the GDPR. See: https://shorturl.at/coBGZ

services" according to Article 6(3) of the e-Privacy Directive,[12] as well as for processing personal location data other than traffic data [Article 9(1) e-Privacy Directive].

Once an online platform begins processing personal data, under EU law it must comply with the remainder of the GDPR in the same way as any other controller or processor. This includes those cases where online platforms are joint controllers with other online services, such as traders[13] provided via the platforms. These cases pose significant challenges as they demand careful analysis of the so-called "boundary resources" (Kurtz et al., 2022) used by platforms to enable the provision of other services, such as apps made available to the users. Analysing the interconnection between the GDPR and the DSA allows us to better understand how protection of personal data applies specifically to online platforms.

Preliminary conclusion to section 2: online platforms and search engines under the DSA are also controllers (and may be processors) under the GDPR, and therefore are required to process personal data in accordance with one or more of the lawful grounds provided for in Article 6(1) GDPR.

3. Protection of personal data and the DSA

In this section, instances of overlap between the GDPR and the DSA are described, classified and analysed in order to provide a framework for online platforms' compliance with data protection duties. There is a distinction made between 1. the general framework of overlap, which includes content moderation and liability as two key pillars of the DSA which are linked to the GDPR, and specific areas of overlap such as 2. personal data protection obligations under the DSA, regarding content moderation and procedural rules, 3. online interface design and organisation prohibitions, 4. profiling prohibitions, and 5. the data protection regulatory approach taken by the DSA.

3.1. General framework: lawful grounds for processing and platform liability

There are numerous references to personal data in the DSA. It is not only referred to in general terms under Recital 10 and Article 2(4)(g), but is addressed in particular under 1. notice and action mechanisms (Recital 52); 2. online advertising (Recitals 68 and 69 and Articles 26, 39 and 46); 3. the protection of minors (Recital 71 and Article 28); 4. the traceability of traders (Recital 72); 5. the definition of active recipients (Recital 77); 6. recommender systems (Recital 94); 7. risk assessment for VLOP and VLOSE (Article 34); 8. research (Recitals 97 and 98); 9. codes of conduct (Recital 103 and Article 45); and 10. enforcement (Recital 148 and Article 40). Many

[12] Directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[13] See article 3(f) DSA.

of these will be discussed below where they provide guidance on interpreting the relevant provisions.

Beyond explicit references to personal data, the DSA implicitly refers to it with respect to two important areas: legal grounds for processing and platform liability. These two areas are interconnected, because the legal basis applicable to personal data processing operations on online platforms give rise to liability in the event of a breach of the GDPR or of other rules on the protection of personal data.

3.1.1. Legal basis for the processing of personal data

The GDPR determines the lawful grounds for the processing of personal data which are applicable to online platforms, as discussed above. The DSA elaborates on these grounds by laying down a set of legal obligations that online platforms are required to comply with and which involve the processing of personal data within the meaning of Article 6(1)(c). This set of obligations comprises: 1. compliance with orders to act against illegal content (Article 9); 2. compliance with orders to provide information (Article 10);[14] 3. management of notice and action mechanisms (Article 16); 4. statement of reasons (Article 17); 5. notifications of suspicion of criminal offences (Article 18); 6. compliance with obligations of traceability of traders (Articles 30 to 32); compliance with investigative and enforcement powers of the Commission in the case of VLOP and VLOSE (Article 40).

This means that where online platforms are concerned, it is necessary to take the DSA into account when assessing and applying the legal basis for the processing of personal data provided for under Article 6(1) of the GDPR. This is especially important because several DSA rules contribute to the application of the principle of purpose limitation.

3.1.2. Platform liability

In addition to the possibility of personal data being used illegally by platforms – i.e. where no lawful ground exists for personal data processing or where prohibited profiling and targeted advertising takes place – it is also possible that third parties, such as traders and other platform users, can use personal data as illegal content, if they access such personal data through the online platform. Given that online platforms process personal data that they use themselves and allow third parties to use, it should be noted that platforms will remain liable for the breach of the GDPR, even where they are not aware that the personal data has been stored on the platform by another recipient of the service – circumstances which would exclude platform liability under the DSA pursuant to Article 6. It is important to distinguish clearly between 1. liability arising from the processing of personal data and the need to comply with the GDPR and other personal

[14] Recital 34 specifically addresses this issue, noting that "the orders should be issued in compliance with Regulation (EU) 2016/679".

data protection legislation, and 2. liability that may arise for online platforms for personal data shared illegally by their users or for breaches of their due diligence obligations under the DSA.

The DSA maintains the rule of exempting online service providers from liability when illegal content is stored without the knowledge of the platform. This has been the rule in the EU (previously under Articles 12 to 14 of the e-Commerce Directive) since 2000 (Farinho & Campos, 2022, pp. 331–348). It is now laid down under Articles 4 to 6 of the DSA (Farinho, 2022, pp. 75–103), although the DSA has added a set of due diligence obligations with which platforms have to comply. This means that online platform liability differs depending on whether it concerns liability for breach of the GDPR or liability for breach of the DSA.[15] In the former case, online platforms are liable for breaches of the GDPR (see Article 82), for example: when personal data is processed without lawful grounds; processing principles are breached; security measures overlooked; or data transfers performed without specific lawful grounds; among other infringements related to online platforms' activities (Eifert et al., 2021, p. 1008). In the latter case, online platforms cannot be held liable for personal data shared by users unless the conditions under Article 6(1) of the DSA apply and the platform has breached their due diligence obligations. It is necessary to maintain this differentiation when applying the DSA.

However, there is one area where there may be an overlap of liabilities under the GDPR and the DSA – where platforms' due diligence obligations under the DSA concern personal data. The DSA gives one example in this area regarding the assessment of systemic risks by Very Large Online Platforms and Very Large Online Search Engines, under Article 34(1)(b) (see Buri, 2023, pp. 80–82).[16] Where VLOP and VLOSE fail to comply with this obligation, they may also be in breach of Article 24(1) and (2) and Article 31 of the GDPR.

Preliminary conclusions to section 3.1: as a general framework, the DSA provides for special cases of legal obligations as lawful grounds for personal data processing, elaborating on the general grounds provided for by Article 6(1)(c) of the GDPR. Data subjects/users, platforms and supervisory authorities should bear these special obligations in mind when determining whether there are lawful grounds for data processing, especially pursuant to Article 6(1)(c).

The DSA also regulates the liability of platforms in cases other than those arising from a breach of the GDPR as controllers (or processors). However, there is one area where liability can overlap, and this occurs when platforms fail to comply with due diligence obligations under the DSA in relation to the protection of personal data.

[15] See EDPS, "Opinion 1/2021 on the Proposal for a Digital Services Act", 2021, pp. 8 and 20.
[16] See Recitals 81 and 94.

3.2. Specific issues: obligations relating to the protection of personal data under the DSA

The DSA is mainly concerned with ensuring that online platforms comply with fundamental rights,[17] since privacy and the protection of personal data occupy a significant place under Articles 7 and 8 of the EU Charter of Fundamental Rights (EUCFR): "This Regulation fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated."[18] Online platforms are a particularly appropriate place to control the exercise of fundamental rights and, given this position, platforms do not only impact upon the exercise of these rights amongst their users, preventing or repressing violations to those rights, but in doing so, they may themselves breach fundamental rights (Egídio, 2022, pp. 217–238). For this reason, the DSA attaches particular importance to online platforms' moderating activities (Quintais et al., 2023): through content moderation, platforms can foster an environment that respects fundamental rights, but they can also restrict those fundamental rights (Gregorio, 2020). It is for this reason that the DSA has introduced procedural rules on how to moderate content and, in doing so, how to privately regulate and enforce fundamental rights (Bassini, 2019, pp. 182–197), including the protection of privacy and personal data (Quintais et al., 2023, pp. 881–911).

3.2.1. Content moderation and procedural rules

Content moderation is legally defined in Article 4(t) of the DSA: "The activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account." In order to moderate content, which, as emphasised above, is also personal data in most cases, it is necessary to process such content within the meaning of Article 4(2) GDPR. Given online platforms' operations and the use of automated systems, it is almost impossible to moderate content without processing at

[17] This concern echoes a similar concern of the United Nations regarding the respect of human rights by online platforms. See United Nations Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 2018. See also Land (2019, pp. 285–316).

[18] See Recital 9.

least some personal data.[19] It is up to those interpreting the law to determine when content moderation constitutes processing of personal data, which is why the due process guaranteed by the DSA toolkit is so important. The DSA aims at making content moderation transparent, pursuant to Articles 14, 15 and 35, in order to facilitate evaluation of compliance with fundamental rights, such as privacy and personal data protection. In the case of VLOP and VLOSE, this goal is clearly stated in the requirements of risk assessment procedures: pursuant to Article 34(1) and (2)(b) these kinds of service providers are required to assess the risk posed by their "content moderation systems" to "the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, *to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter,* to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter" (emphasis added). This means that the DSA requires online platforms to respect the right to privacy and the right to the protection of personal data in accordance with the GDPR, when applying their terms and conditions to users pursuant to Article 14(1) and (4).[20]

Content moderation, as envisaged by the DSA and viewed from the perspective of the GDPR and data protection, is as much an activity destined to protect the fundamental rights of users from other users and public authorities, as it is a means to protect users from the platform itself. This latter aspect is the essence of Article 14(4) of the DSA: any restrictions imposed on users by online platforms in the name of terms and conditions and enforced through content moderation mechanisms has to comply with fundamental rights (Quintais et al., 2023, pp. 881–911), and this involves protecting users both from public power and the power of the platforms.[21] Online platforms are called upon to perform a balancing act between the conflicting fundamental rights identified through content moderation mechanisms (Eifert et al., 2021, p. 1011). Content moderation includes taking down illegal content, as identified by the platforms, their users (including trusted flaggers pursuant to Article 22 of the DSA) and EU or EU Member States authorities. This is another area of overlap with the GDPR, given that orders to act against illegal content (Article 9 DSA) and notice and action mechanisms (Article 16 DSA) can be used to act against violations of the GDPR (as illegal content), or to exercise rights laid down in the latter regulation. An important example is the exercise of the right to erasure under the GDPR [see Article 17(1)(d)] vis-à-vis the notice and action mechanism against illegal use of a platform user's personal data [Article 16(1) DSA].

[19] See EDPS Opinion 1/2021 p. 10: "The EDPS wishes to underline that depending on the categories of data that are processed and nature of the processing, automated content moderation may significantly impact both the right to freedom of expression and the right to data protection."

[20] See Recitals 45 to 47.

[21] On the human/fundamental rights framework of online platforms regarding content moderation, see Jørgensen (2019, p. 181).

The DSA provides a set of procedural rules to underpin these balancing operations, but does not create new substantive rules to prevent or resolve such conflicts; rather, the DSA relies on a general reference to "illegal content"[22] as defined by EU and Member State law. Thus, the DSA focuses on procedural rules when dealing with content moderation. This is the case with 1. transparency reporting obligations, 2. notice and action mechanisms, 3. duty to state reasons, 4. use of internal complaint-handling systems and 5. out-of-court dispute settlements, as well as reliance on 6. trusted flaggers, 7. recommender system transparency, 8. traceability of traders, and, in the case of VLOP and VLOSE, 9. risk assessment and 10. measures to mitigate risks. This procedural toolkit also applies to the enforcement of the right to protection of personal data. The bottom line is that the DSA defines a specific type of personal data processing operation – content moderation – with the aim of ensuring that such processing complies with the fundamental rights to privacy and data protection and, consequently, with the GDPR.

Understanding content moderation as a specific type of personal data processing is important for those interpreting the law and for other legal practitioners, from platform lawyers to consumer association lawyers and, of course, supervisory authorities and judges. This is because content moderation's status as personal data means that content moderation due diligence rules under the DSA have to be applied in accordance with the GDPR, and any breach may also entail a breach to the GDPR.

3.2.1.1. Automated processing of personal data

Among the forms of content moderation, one type in particular deserves special attention from the EU legislator: automated processing. This is because this type of content moderation, which at least in its early stages does not involve human intervention, can lead to a range of problems ranging from classification errors to decision bias.[23] Concerning automated processing of personal data and especially in the case of content moderation, an interesting dialogue has been established between the GDPR and the DSA.

The DSA presupposes that online platforms use automated tools to some extent in order to moderate content (Recital 26). Under the GDPR, a particularly restrictive approach to automated personal data processing can be observed. Article 22(1) states that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[24] However, exceptions from Article 22(2) apply, which include: 1. where necessary to enter into or perform a contract, 2. authorisation by the Union or Member State law, or 3. explicit consent. This appears to mean that the data subject/user can object to the use of any content moderation tool by online platforms where it involves the processing of personal data, unless one of the

[22] For the DSA definition of illegal content see Article 3(h).

[23] See Article 29 Working Party, "Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679", adopted on 3 October 2017, and later adopted by the EDPB.

[24] See also Recital 71.

exceptions to Article 22(1) applies. As mentioned above, not all content moderation involves personal data processing, and this may explain the duties foreseen under Articles 14(1), 15(b), (c) and (e), 16(6) and 17(3)(c) of the DSA for online platforms to: 1. inform users, through their terms and conditions of any "policies, procedures, measures and tools used for the purpose of content moderation including algorithmic decision-making and human review"; 2. include in their transparency reports information on the use of automated content moderation tools;[25] 3. disclose the use of any automated means for processing or decision-making regarding notices of illegal content; and 4. include in their statement of reasons regarding any restrictions imposed on users "information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means".[26] This information is the only way for users to be able to exercise the right to object to such automated personal data processing and for administrative authorities to be able to assess compliance with the DSA.[27] Lastly, the DSA forbids decisions issued from the mandatory internal complaint-handling system to be based solely on automated means, pursuant to Article 20(6). Although these decisions may not relate directly to content moderation, they are connected with it inasmuch as most of these decisions are taken by the provider of the online platform following content moderation, as follows from Article 20(1) of the DSA.

As part of this discussion, it is necessary to consider a third piece of legislation which will have the greatest impact on the automated processing of personal data in online platforms' content moderation mechanisms: the AI Act.[28] The Act had not yet been published at the time of this paper's submission for publication. However, during the negotiations among EU legislators, the issue of "consistency with the GDPR" was raised.[29] This is understandable as many online platforms use AI to perform content moderation operations. Insofar as these algorithms process personal data, they are subject to both the GDPR and the DSA, as well as the future AI Act (Pollicino & Gregorio, 2022, pp. 8–9).

Preliminary conclusion to section 3.2: The focus of the DSA on content moderation and the procedural rules that frame such moderation should remind those interpreting the law that content moderation can be a type of personal data processing, and that, therefore, the procedural rules applicable to content moderation can function as specific rules applying to the obligations of the controller when personal data is processed. This is clear in the case of assessment of impact on fundamental rights, both in terms of content moderation and personal data processing. Therefore, GDPR and the DSA have to be applied in tandem whenever platforms are involved, and those interpreting the law will

[25] See EDPS Opinion 1/2021 p. 12.

[26] EDPS Opinion 1/2021 p. 12.

[27] See also Recitals 54 and 58 of the DSA; see Eifert et al. (2021, p. 1016).

[28] Proposal 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, COM(2021) 206 final, 2021/0106(COD); latest version used (30 April 2024) available at: www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

[29] See European Parliament, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD))" of 20 April 2022, p. 157.

need to determine which obligations are relevant to content moderation as personal data processing, and how.

3.3. Specific issues: online interface design and organisation prohibitions

The DSA adds another layer of protection concerning manipulative or deceptive design, also known as dark patterns (Becker & Penfrat, 2023, pp. 56–57). As the EDPB reminds us, "[t]he GDPR's provisions apply to the entire course of personal data processing as part of the operation of social media platforms, i.e. to the entire life cycle of a user account",[30] and thus many deceptive practices in both the design and organisation of platform interfaces infringe the GDPR.[31] The DSA, while not laying down special rules which would affect those applicable in the GDPR – this is explicitly acknowledged under Article 25(2) of the DSA – provides a layer of rules of its own, prescribing, pursuant to Article 25(1) that platforms "shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".[32] In practice, this means that while the GDPR covers most deceptive patterns that involve personal data, especially given the guidance provided by the EDPB, the DSA will cover all remaining user interactions, where personal data is not present or where personal data is present but no provision from the GDPR covers that specific case. It is of utmost importance that further work is done by those interpreting the law, from scholars to supervisory authorities and courts, to determine whether and in what cases personal data may be protected by the DSA, rather than the GDPR, from the dark patterns in platforms' interfaces. That said, although the DSA provision regarding dark patterns most likely will not directly affect the protection of personal data, it may play a role in preventing or mitigating cases directly protected by the GDPR. This is something that must be taken into consideration by consumers and consumer associations when protecting the status of platform users.

Preliminary conclusion to section 3.3: While not providing for special rules prohibiting dark patterns regarding the use of personal data, the DSA provides for a comprehensive prohibition on dark patterns regarding non-personal data that could work to prevent, mitigate or reinforce the protection of personal data against dark patterns covered by the GDPR, as well as in cases where the GDPR does not apply.

3.4. Specific issues: profiling prohibitions

Amongst other functions, the DSA reflects the EU's vision on how personal data is used by online platforms and endeavours to address those aspects of data processing, with

[30] See EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, adopted on 14 February 2023, p. 4.

[31] See EDPB Guidelines 03/2022 for several examples of online platforms' practices infringing the GDPR.

[32] See also Recital 67.

"profiling" centre stage as the main villain (Büchi et al., 2020). On the one hand, online platforms use personal data to personalise user experience, thus making the service more enticing, but also to monitor their actions and thus improve content moderation. On the other hand, such personal data and its findings can be used to offer better advertising services to companies, which in turn aim to reach potential clients more effectively. These two dimensions are clearly in the crosshairs of the DSA, and there was already an awareness of them prior to the enactment of the DSA. The European Data Protection Supervisor (EDPS), in his assessment of the DSA proposal, stressed that the three key areas of concern should be 1. content moderation; 2. online advertising; and 3. recommender systems.[33] Having analysed content moderation, online advertising and recommender systems will now be addressed.

3.4.1. Online advertising

Online advertising is the first domain in the DSA where one finds explicit and specific rules concerning the GDPR. Article 26(3) determines that "[p]roviders of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679". This rule was not in the EU Commission's original proposal, only being added after the amendments proposed by the EU Parliament.[34] This prohibition is composed of three elements. It addresses 1. targeted advertisement, 2. profiling and 3. sensitive personal data. In this sense, it combines three of the main concerns of the DSA and the GDPR.

Targeted advertising is not prohibited by either the GDPR or the DSA (except in the case of minors, see below) and the same can be said for profiling, although it raises several issues regarding online platforms in particular.[35] Given the high risk of targeted advertising on online platforms, the EDPB suggested the "prohibition of targeted advertising on the basis of pervasive tracking",[36] although this was not included in the final version of the DSA. Profiling is one of the major concerns of the GDPR,[37] warranting 1. a definition under Article 4(4) (Bygrave, 2020, pp. 125–131; Scholz, 2019, pp. 306–311; for profiling in general see Hildebrandt & Gutwirth, 2008), 2. specific rights to object to processing when profiling is involved, pursuant to Article 21(1) and (2) and 3. a right of the data subject "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly

[33] See EDPS Opinion 1/2021 p. 3.

[34] See European Parliament Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available online at: www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html

[35] See EDPB Guidelines 8/2020 on the targeting of social media users, Version 2.0 Adopted on 13 April 2021, pp. 5 and ff.

[36] EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, p. 2.

[37] See EDPB Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018); see CJUE Decision C-252/21, *Bundeskartellamt*, 04.11.2023, ECLI:EU:C:2023:537.

affects him or her", under Article 22(1), with the exceptions provided for in paragraph (2).[38] On the other hand, sensitive data is highly protected in the DSA, its processing being forbidden by default under Article 9(1), with the exceptions in paragraph (2). This means that prior to the DSA and under the GDPR, online platforms could indeed perform targeted advertising based on profiling if one of the exclusions in Article 9(2), namely consent, applied. Thus, the rule in Article 26(3) of the DSA is a specific rule concerning the processing of sensitive personal data for targeted, profiled advertising. It can be said that whereas the GDPR and the e-Privacy Directive did not prohibit profiling based on personal data or the processing of personal data for targeted advertising – instead providing for the right to object [Article 21(2) GDPR] or consent-only advertising [Article 6(3) e-Privacy Directive] – the DSA now prohibits both when sensitive data is involved.[39] Taking into account that online targeted advertising relies heavily on sensitive data to profile users and better target ads, this was a compromise by the DSA legislator to prevent a complete ban on targeted advertising.[40]

This rule is especially important as a tool to fight dark patterns on online platforms (Valcke et al., 2022, p. 61). As can be read in Recital 69: "When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups."[41]

3.4.2. Protection of minors

A similar rule to that of Article 26(3) DSA can be found in Article 28(2) regarding the protection of minors: "Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor." Following the EDPB,[42] the DSA legislator again prohibits targeted advertising, in this case towards minors, if profiling based on their personal data is taking place. The subjective scope of the rule is narrower than that of Article 26(3) DSA, although wider in its objective scope: the rule applies only to minors and not to any online platform user, but the prohibition now extends to all targeted advertising based on the profiling of any personal data and not only that of a sensitive nature within the meaning of Article 9(1) of the GDPR.

There is no reference to minors in the GDPR, "children" being the preferred term of the legislator to address the concerns relating to minors. However, the two words do not have the same legal meaning. Minors in all EU legal systems are those data subjects who,

[38] On interpretative problems arising from Article 22(1) see Binns and Veale (2021, pp. 319–332).
[39] See Recital 68.
[40] Calling it a "half-baked restriction", see Becker and Penfrat (2023, p. 58).
[41] See EDPB Guidelines 03/2022 pp. 25 and 42 for some examples concerning advertising.
[42] See EDPB, "Statement on the Digital Services Package and Data Strategy", p. 3.

because of their age, do not yet have full legal capacity, even if the legal age of full capacity varies from country to country.[43] This difference is of relevance, not only because the DSA prefers the wording "minor", but because in the GDPR children can exert consent, regarding "information society services" when they are sixteen years old, or less if explicitly provided for under national law, according to Article 8(1).[44] This is an especially relevant provision of the GDPR as it is linked to Article 28(2) of the DSA: the DSA prevents online platforms from exposing children – as minors – to profiled targeted advertising, notwithstanding (and, one might add, especially in light of) the fact that children can consent to the use of online platforms from the age of 16.[45]

The legislator was cautious in the way it constructed this rule: 1. it applies not only in cases where online platforms know that the users are minors but also 2. in the cases where there is a "reasonable certainty" that the targeted users are minors. Such "reasonable certainty" does not demand that the online platforms process additional personal data in order to confirm whether the user is a minor [Article 28(3) DSA]. As mentioned in Recital 71, Article 28(2) "should not incentivize providers of online platforms to collect the age of the recipient of the service prior to their use".

3.4.3. Recommender systems

The DSA addresses recommender systems[46] regarding all online platforms under Article 27[47] but it lays down a specific rule for VLOP and VLOSE concerning the protection of personal data: "Providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679" (Article 38).[48] Again, profiling is targeted by the legislator and again following a suggestion by the EDPB.[49] In this case, profiling is not prohibited *per se*. What is prohibited is that online platform users be subjected exclusively to recommender systems based on profiling.[50] This means that the exclusive use of profiling as the basis for recommender systems is prohibited; this is another sign of the EU's stance on the harm that profiling can cause. In this case, this entails a restriction on the use of personal data, provided for outside of the GDPR, but in accordance with GDPR Articles 21 and 22.

[43] All EU Member States foresee eighteen as the age in which full legal capacity is acquired.

[44] For instance, under Portuguese law the age of consent regarding children is thirteen, pursuant to Article 16(1) of Law n.º 58/2019, of 8 August.

[45] See Recital 71 and its reference to "EU Better Internet for Kids strategy (BIK+)".

[46] For the legal definition of the DSA, see Article 3(s).

[47] See Recital 70.

[48] See Recital 94.

[49] EDPB Statement on the Digital Services Package and Data Strategy, p. 6.

[50] The EDPS not only suggested that "recommender systems should by default not be based on 'profiling' within the meaning Article 4(4) of Regulation (EU) 2016/679" but it also "strongly recommend[ed] to modify the requirement to opt-in rather than opt-out, making the option not based on profiling the default one". See EDPS, Opinion 1/2021, pp. 16 and 17.

Preliminary conclusions to section 3.4: The EU legislator appears to have used the DSA to go one step further in the treatment given by the GDPR to the profiling and targeting of data subjects. In all the instances where the DSA addresses these activities, it increases data protection by restricting profiling and targeting activities. It forbids targeted advertising using profiles based on sensitive personal data; it prohibits targeted advertising to minors based on profiling; and finally, concerning VLOP and VLOSE, it prohibits platforms from offering exclusively profiling-based recommender systems, obliging them to offer a non-profiled alternative.

3.5. The DSA data protection regulatory approach

In addition to the substantive and procedural rules analysed so far, there is a third important dimension to data protection in the DSA: the institutional regulatory framework (Eifert et al., 2021, p. 994). EU legislators have not only 1. created new national regulators – the Digital Services Coordinators[51] –, which have a duty to cooperate with each other pursuant to Article 58, but have also 2. envisaged a European Board for Digital Services, as an "independent advisory group of Digital Services Coordinators".[52] Last but not least, 3. the EU legislator has appointed the EU Commission as the enforcement authority for the DSA with respect to VLOP and VLOSE[53] (except for the provisions of Chapter III, Sections 1, 2, 3, where competence remains with the Digital Services Coordinators). Given the systemic risks posed by these very large service providers, the DSA requires that they perform a risk assessment covering, among other risks, "any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter" [Article 34(1)(b)]. Additionally, the DSA foresees a "crisis response mechanism" (Article 36) under which the Commission may define a set of measures to be applied by online platforms in order to mitigate or end a crisis.

The regulatory power conferred upon the new Digital Services Coordinators and the Commission is very extensive and focuses on the protection and enforcement of fundamental rights, where the protection of personal data is involved. As regards Digital Services Regulators, in Article 51 the DSA provides for 1. powers of investigation [paragraph (1)] and 2. powers of enforcement [paragraphs (2) and (3)]. The powers of investigation cover the inspection of content moderation procedures used by online platforms. As we have seen above, this involves the inspection of any personal data processing operations that may breach both the DSA and the GDPR. It follows that the regulatory institutional structure put in place by the DSA also regulates and enforces data protection when intermediary service providers are involved, as is the case with

[51] See Articles 49 to 51.

[52] See Article 61(1).

[53] See Articles 65 and ff. Also, on the status of the Commission as VLOP and VLOSE regulator, see Buri (2023, pp. 80–82).

online platforms. Here again, there is supposed to be an emphasis on the collaborative mechanism between the two institutional regulatory frameworks, especially between national data protection supervisory authorities and the new Digital Services Coordinators. When it comes to the Commission in respect of VLOP and VLOSE, the DSA also foresees extensive 1. investigatory powers (Articles 65 to 69) and 2. enforcement powers (Articles 70 to 76). Again to a great extent, this regulatory apparatus will have to focus on the protection of personal data,[54] in cooperation with the national supervisory authorities for the protection of personal data under the GDPR. This cooperation will be essential in order to adequately enforce personal data protection rules regarding online platforms:[55] many of the procedures foreseen in the DSA – pertaining to access to information via reports and other documents, giving reasons for the restriction of content, use of complaint and out-of-court dispute mechanisms – are a pre-condition for the use of complaint mechanisms under the GDPR and via the national data protection authorities. Information gathered from the DSA will support the procedures under the GDPR.[56]

Preliminary conclusions to section 3.5: In addition to the due diligence obligations set forth in the DSA, the institutional apparatus established by the DSA plays a significant role not only in platform regulation, but also in personal data protection. Given the fact that the digital services coordinators provided for in the DSA will act as special data protection regulators in addition to the general data protection regulators provided for in the GDPR, it becomes obvious that there will be a need for coordination. Such coordination needs to take place at three different levels: 1. within EU Member States between the GDPR supervisory authority and the DSA digital services coordinators, 2. among EU Member States concerning the result of internal coordination, and, regarding VLOPs and VLOSEs, 3. between the Commission and EU Member States. This results in a complex institutional system that will need to be carefully planned and monitored by each Member State and the Commission.

4. Conclusions

The main claim of the paper is that on the one hand, the DSA assumes the role of *lex specialis* vis-à-vis the GDPR, but on the other it also complements the GDPR; this calls for an analysis of 1. specific legal grounds for data processing in compliance with platforms' new legal obligations, 2. a new articulation between both regulations concerning dark patterns, 3. new prohibitions on personal data processing, 4. new obligations to protect personal data, and 5. a new ancillary institutional framework to

[54] See Recital 103.

[55] The EDPB has stressed the importance of this interplay and the lack of proper, formal mechanisms of cooperation. See EDPB, Statement on the Digital Services Package and Data Strategy, pp. 3 and 4; see also Jaursch (2023, pp. 95–96).

[56] This is especially important given the fact that most EU Member States have designated as their Digital Services Coordinator, in line with what had happened under the transposition of the e-Commerce Directive, their telecoms regulators and not their data protection supervisory authorities under the GDPR.

regulate data protection by online platforms in collaboration with national data protection authorities. Online platforms and search engines under the DSA are also controllers (and may be processors) under the GDPR and are, therefore, required to process personal data under one or more of the legal basis provided for by Article 6(1) GDPR. The DSA provides for special cases of legal obligations as legal grounds for personal data processing, thus elaborating on the general ground provided for by Article 6(1)(c) of the GDPR. Data subjects/users, platforms and supervisory authorities should bear these special obligations in mind when determining whether there are lawful grounds for data processing, especially pursuant to Article 6(1)(c). The DSA also covers cases of platform liability which differ from the liability arising from the breach of the GDPR as controllers (or processors), and this should be taken into consideration when assessing how platforms handle personal data. However, there is one area where liability can overlap, and this occurs when platforms fail to comply with due diligence obligations under the DSA regarding the protection of personal data. The DSA's focus on content moderation and procedural rules that frame such moderation activity must remind the interpreters of law that content moderation can be a type of personal data processing and, therefore, procedural rules applicable to content moderation may work as special rules concerning duties of the controller when processing personal data. This is clear in the case of fundamental rights impact assessment, both on content moderation and personal data processing. The GDPR and the DSA must, therefore, be used together, whenever platforms are involved and the interpreter wants to determine which duties apply (and how) to content moderation as personal data processing. Starting from this general framework, a set of specific areas where the DSA is linked to the GDPR were identified and analysed.

While not providing for special rules on the prohibition of dark patterns to be aligned with the provisions of the GDPR, it does provide for a comprehensive prohibition on dark patterns that may work to prevent, mitigate or reinforce the protection of personal data regarding dark patterns provided for by the GDPR or in cases where the GDPR does not apply.

The EU legislator seems to have used the DSA to go one step further in the treatment given by the GDPR to the profiling and targeting of data subjects. In all the instances where the DSA addresses these activities, it increases data protection by restricting profiling and targeting activities. It forbids targeted advertising using profiles based on sensitive personal data, it prohibits targeted advertising to minors based on profiling, and finally, concerning VLOP and VLOSE, it prohibits platforms from offering exclusively profiling-based recommender systems, creating a duty to offer a non-profiled alternative.

Finally, in addition to the due diligence duties set forth in the DSA, the institutional apparatus designed by the DSA plays a significant role not only in platform regulation but in its interplay with personal data protection. Given the fact that the digital services coordinators foreseen in the DSA will act as special data protection regulators in addition to the general data protection regulators foreseen in the GDPR, the need for coordination becomes obvious. This coordination will have to be done at three different levels: 1. within EU Member States between the GDPR supervisory authority and the DSA digital services coordinators, 2. among EU Member States concerning the result of internal coordination,

and, regarding VLOP and VLOSE, 3. between the Commission and EU Member States. This results in a complex institutional arrangement that must be carefully planned and monitored by each Member State and the Commission.

The analysis presented in this paper shows that personal data protection continues to exhibit a radiant effect stemming from the GDPR towards new legislation enacted by the European Union. The DSA is one of the most recent examples of this effect (as is the upcoming AI Act), and it is an especially important one as this regulation deals with everyday interactions on the Internet, through online platforms. Concerning data protection, the analysis performed showed that there are several areas where the GDPR and the DSA meet and the actors in the legal chain related to personal data protection compliance and enforcement can use the present work as a tool to interpret and apply the combination of GDPR and DSA provisions regarding the protection of personal data on online platforms. The analysis also shows, however, that there are some areas – like dark patterns, exercise of rights and institutional articulation – where the interaction between the GDPR and the DSA will require further elaboration from supervisory authorities, the EDPB, the new European Board for Digital Services, the Commission and the courts, with special emphasis on the CJEU. Further work of scholars and practitioners within a framework of the identified areas of interaction can undoubtedly help this endeavour.

Acknowledgments

The author wishes to express his thanks to the two anonymous reviewers and to the participants of the Lisbon Digital Rights Research Group's (Lisbon Public Law, University of Lisbon) Workshop on Ongoing Work (May 2023) for all their comments on and suggestions for a previous version of the paper.

References

Bassini, M. (2019). Fundamental Rights and Private Enforcement in the Digital Age. *European Law Journal, 25*(2), 182–197. Online: https://doi.org/10.1111/eulj.12310

Becker, S. & Penfrat, J. (2023). Still Useful. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri & M. Straub (Eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications* (pp. 51–62). Verfassungsbooks. Online: https://doi.org/10.17176/20230208-093135-0

Binns, R. & Veale, M. (2021). Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR. *International Data Privacy Law, 11*(4), 319–332. Online: https://doi.org/10.1093/idpl/ipab020

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S. & Viljoen, S. (2020). The Chilling Effect of Algorithmic Profiling: Mapping the Issues. *Computer Law & Security Review, 36.* Online: https://doi.org/10.1016/j.clsr.2019.105367

Buri, I. (2023). A Regulator Caught Between Conflicting Policy Objectives. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri & M. Straub (Eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications* (pp. 75–90). Verfassungsbooks. Online: https://doi.org/10.17176/20230208-093135-0

Bygrave, L. (2020). Commentary to Article 4(4). In C. Kuner, L. A. Bygrave & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 125–131). Oxford University Press. Online: https://doi.org/10.1093/oso/9780198826491.003.0010

Dijck, J. van, Poell, T. & Waal, M. de (2018). *The Platform Society. Public Values in a Connective World*. Oxford University Press. Online: https://doi.org/10.1093/oso/9780190889760.001.0001

Egídio, M. M. (2022). Social Networks and the Exercise of Fundamental Rights: Public Administration and the Digitalization of Fundamental Rights. In C. B. de Morais, G. F. Mendes & T. Vesting (Ed.), *The Rule of Law in Cyberspace* (pp. 217–238). Springer. Online: https://doi.org/10.1007/978-3-031-07377-9_12

Eifert, M., Metzger, A., Schweitzer, H. & Wagner, G. (2021). Taming the Giants: The DMA/DSA Package. *Common Market Law Review, 58*(4), 987–1028. Online: https://doi.org/10.54648/cola2021065

Farinho, D. S. (2022). Fundamental Rights and Conflict Resolution in the Digital Services Act Proposal: A First Approach. *e-Pública, 9*(1), 75–103. Online: https://shorturl.at/ijAQR

Farinho, D. S. & Campos, R. R. (2022). Models of Legal Liability for Social Networks: Between Germany and Portugal. In C. B. de Morais, G. F. Mendes & T. Vesting (Eds.), *The Rule of Law in Cyberspace* (pp. 331–348). Springer. Online: https://doi.org/10.1007/978-3-031-07377-9_17

Goldman, E. (2020). An Overview of the United States' Section 230 Internet Immunity. In G. Frosio (Ed.), *The Oxford Handbook of Online Intermediary Liability* (pp. 155–171). Oxford University Press. Online: https://doi.org/10.1093/oxfordhb/9780198837138.013.8

Gregorio, G. De (2020). Democratising Online Content Moderation: A Constitutional Framework. *Computer Law & Security Review, 36.* Online: https://doi.org/10.1016/j.clsr.2019.105374

Hartmann, I. A. (2020). A New Framework for Online Content Moderation. *Computer Law & Security Review, 36.* Online: https://doi.org/10.1016/j.clsr.2019.105376

Hildebrandt, M. & Gutwirth, S. (Eds.) (2008). *Profiling the European Citizen.* Springer. Online: https://doi.org/10.1007/978-1-4020-6914-7

Jaursch, J. (2023). Platform Oversight. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri & M. Straub (Eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications* (pp. 91–106). Verfassungsbooks. Online: https://doi.org/10.17176/20230208-093135-0

Jørgensen, R. F. (2019). Rights Talk. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 163–188). MIT Press.

Klonick K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review, 131*(6), 1598–1670. Online: https://shorturl.at/bnEO3

Kosseff, J. (2016). The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution Over Two Decades. *The Columbia Science & Technology Law Review, 18*(1), 1–41. Online: https://doi.org/10.7916/stlr.v18i1.4011

Kurtz, C., Wittner, F., Semmann, M. & Schulz, W. (2019). The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems. *Proceedings of the 52nd Hawaii International Conference on System Sciences,* 52, pp. 5059–5068.

Kurtz, C., Wittner, F., Semmann, M., Schulz, W. & Böhmann, T. (2022). Accountability of Platform Providers for Unlawful Personal Data Processing in Their Eco-Systems – A Socio-Techno-Legal Analysis of Facebook and Apple's iOS According to the GDPR. *Journal of Responsible Technology, 9.* Online: https://doi.org/10.1016/j.jrt.2021.100018

Land, M. K. (2019). Regulating Private Harms Online: Content Regulation under Human Rights Law. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 285–316). MIT Press.

Pollicino, O. & Gregorio, G. De (2022). Constitutional Law in the Algorithmic Society. In H.-W. Micklitz, O. Pollicino, A. Simoncini, G. Sartor & G. De Gregorio (Eds.), *Constitutional Challenges in the Algorithmic Society* (pp. 3–24). Cambridge University Press. Online: https://doi.org/10.1017/9781108914857.002

Quintais, J. P., Appelman, N. & Ó Fathaigh, R. (2023). Using Terms and Conditions to Apply Fundamental Rights to Content Moderation. *German Law Journal, 24*(5), 881–911. Online: https://doi.org/10.1017/glj.2023.53

Scholz, P. (2019). Kommentar zum artikel 4 Nr. 4. In S. Simitis, G. Hornung & I. g. D. Spiecker (Eds.), *Datenschutzrecht. DSGVO mit BDSG* (pp. 306–311). Nomos.

Taddeo, M. & Floridi, L. (2017a). New Civic Responsibilities for Online Service Providers. In M. Taddeo & L. Floridi (Eds.), *The Responsibilities of Online Service Providers* (pp. 1–10). Springer. Online: https://doi.org/10.1007/978-3-319-47852-4_1

Taddeo, M. & Floridi, L. (2017b). The Moral Responsibilities of Online Service Providers. In M. Taddeo, L. Floridi (Eds.), *The Responsibilities of Online Service Providers* (pp. 13–42). Springer. Online: https://doi.org/10.1007/978-3-319-47852-4_2

Turillazzi, A., Taddeo, M., Floridi, L. & Casolari, F. (2023). The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications. *Law, Innovation and Technology, 15*(1), 83–106. Online: https://doi.org/10.1080/17579961.2023.2184136

United Nations Human Rights Council (2018). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

Valcke, P., Clifford, D. & Dessers, V. K. (2022). Constitutional Challenges in the Emotional AI Era. In H.-W. Micklitz, O. Pollicino, A. Simoncini, G. Sartor & G. De Gregorio (Eds.), *Constitutional Challenges in the Algorithmic Society* (pp. 57–77). Cambridge University Press. Online: https://doi.org/10.1017/9781108914857.005

Wischmeyer, T. (2020). What is illegal offline is also illegal online: the German Network Enforcement Act 2017. In B. Petkova & T. Ojanen (Eds.), *Fundamental Rights Protection Online* (pp. 28–56). Edward Elgar Publishing. Online: https://doi.org/10.4337/9781788976688.00012

York, J. C. & Zuckerman, E. (2019). Moderating the Public Sphere. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 137–162). MIT Press.