Searching for Coordination between the EU Copyright Enforcement System and Content Portability: An Underestimated Challenge?

by

Camilla Signoretta*

CONTENTS

Abstract

Portability is a multifaceted concept, standing in between data law, digital consumer law and platform regulation. Considering their different rationale, portability rules can be found in the General Data Protection Regulation (GDPR), the Digital

* Camilla Signoretta, PhD in Law, Scuola Superiore Sant'Anna, Pisa, Italy; e-mail: camilla.signoretta@santannapisa.it; ORCID: https://orcid.org/0009-0009-4799-3787.

Suggested Citation: Camilla Signoretta, 'Searching for Coordination between the EU Copyright Enforcement System and Content Portability: An Underestimated Challenge?' (2024) 17 YARS pp. 175–207.

Article received: 8 January 2024, accepted: 29 May 2024.

Yearbook of Antitrust and Regulatory Studies, Vol. 17, No. 29, pp. 175–207 • ISSN 1689-9024
https://doi.org/10.7172/1689-9024.YARS.2024.17.29.6

Content Directive (DCD), the Portability Regulation (PR), and the Digital Markets Act (DMA). Throughout the years, portability evolved from a prerogative of data subjects into a content regulatory tool. Therefore, its interplay with intellectual property law became progressively more complicated. Importantly, some portability provisions have been enacted in the form of obligations to be implemented by digital platforms. In this light, the intersection between digital platform regulation and portability may raise concerns. In particular, the relationship between portability and Article 17 of the Copyright Digital Single Market Directive (CDSMD) deserves particular attention. The high liability threshold set therein, and the structural deficiencies of this provision, risk pushing providers towards hyper-deterrent strategies to avoid liability, with the collateral risk of under-implementing portability duties.

Résumé

La portabilité est un concept à multiples facettes, qui se situe entre le droit des données, la loi sur la consommation numérique et la réglementation des plateformes. Compte tenu de leurs différentes de la protection des données (GDPR), la directive sur le contenu numérique (DCD), la directive sur le contenu numérique (DCD), le règlement sur la portabilité (PR) et la loi sur les marchés numériques (Digital Markets Act). Au fil des ans, la portabilité a évolué, la portabilité a évolué d'une prérogative des personnes concernées à un outil de réglementation du contenu. Par conséquent, son interaction avec le droit de la propriété intellectuelle est devenue de plus en plus compliquée. Il est important de noter que certaines dispositions relatives à la portabilité ont été adoptées sous la forme d›obligations à mettre en œuvre par les plateformes numériques. Dans ce contexte, l›intersection entre la réglementation des plateformes numériques et la portabilité peut soulever des préoccupations. En particulier, la relation entre la portabilité et l'article 17 de la directive sur le marché unique du droit d'auteur (CDSMD) mérite une attention particulière. Le seuil de responsabilité élevé qui y est fixé et les déficiences structurelles de cette disposition risquent de pousser les utilisateurs à se tourner vers des strategies hyper dissuasives pour éviter la responsabilité, avec le risque collatéral d'une mise en œuvre insuffisante des obligations de portabilité.

Key words: digital platform regulation; consumer protection; intermediary liability; copyright enforcement; portability.

JEL: K12, K21, K29

I. Introduction

Portability emerged as a service which allows data to migrate from a provider to a new one. This is the way cloud storage services function, helping data to freely circulate among providers, without losing content through the act of switching. Yet, the concept of portability changed throughout the years from a legal tool in the hands of data subjects towards a pro-competitive instrument useful to regulate digital markets. In this respect, it underwent a metamorphosis in nature, standing at the borderline of the European Union (EU) data protection law, competition law and digital consumer law. In this way, portability evolved into a multifaceted content-regulating tool, with an impact on EU digital platform regulation.

The paper starts with an overview of Article 20 of the General Data Protection Regulation (hereinafter: GDPR) (**II**), conferring upon data subjects the all-encompassing prerogative of "porting" their personal data to a new provider. The analysis will focus on the merits and limits of this provision, subject to several applicability conditions, and full of ambiguities as to its scope and interplay with intellectual property rights (hereinafter: IPRs). Attention will then be shifted to Article 16 of the Digital Content Directive (hereinafter: DCD) (**III**). This provision contains a portability remedy operating upon the termination of contracts for the supply of digital content or services. The analysis will proceed to point out divergences in scope and purpose between Article 16 DCD and Article 20 GDPR, with specific regard to the peculiar role played by portability as a contract law remedy in Article 16 DCD. In particular, the focus will be placed on the relationship between portability and IPRs, in order to understand whether the latter may hamper the effectiveness of the former in the case of mixed datasets.

Thereafter, the Portability Regulation (hereinafter: PR) will be analysed (**IV**), with specific reference to the portability obligation embedded in Article 3 PR. Concerning this provision, the paper will outline the different attitudes endorsed by the EU legislator towards the delicate relationship with IPRs, explaining why it can be considered more advanced than previously discussed portability rules. Afterwards, the newly enacted portability obligations for gatekeepers under Articles 6(9) and 6(10) of the Digital Markets Act (hereinafter: DMA) will be discussed in depth (**V**). Specifically, the focus will be put on the similarities with Article 20 GDPR in terms of their rationale and look at the consequences stemming from the under-implementation of DMA portability obligations.

After completing this extensive portrait of the portability provisions scattered in EU law, the paper will explore their relationship with the

copyright enforcement system, also investigating its impact on the liability of digital platforms (**VI**). In this sense, the analysis will seek to understand how to strike a balance between portability and the necessity of granting adequate protection to IP rightsholders. To do so, the interplay between portability and Article 17 of the Copyright Digital Single Market Directive (hereinafter: CDSMD) will be assessed. The complexities of Article 17 CDSMS will be explored, which establishes a two-tiered copyright infringement liability system for content providers and is full of implications for the digital ecosystem. The emphasis will be placed on the unclear liability threshold set within the text of this controversial provision, arguing whether it incentivizes the adoption of technologies filtering online content *ex-ante*, ultimately hindering portability.

II. From (Personal) Data Portability…

Portability first emerged as an instrument to enhance data subjects' control over personal data during automated processing. Accordingly, the data subject has the prerogative of receiving personal data concerning them and transmitting it to another controller in a specific format. Thus, Article 20 GDPR encapsulates a specific notion of portability, characterised by a consumer law trait.[1] Portability also seeks to reduce switching costs of data transfers, and to keep the level of competition high in data-driven markets.[2] Hence, new entrants in the platform market do not face excessive entry barriers, and are not diluted by *lock-in* effects.[3] By increasing control over personal data,[4]

[1] S Geiregat, 'Copyright Meets Consumer Data Portability Rights: Inevitable Friction between IP and the Remedies in the Digital Content Directive' (2022) 71(6) GRUR International 495–515.

[2] Communication from the Commission, Strategy for Europe's Digital Single Market, COM (2015), 0192 final, § 4.1.

[3] T Tombal, 'Imposing Data Sharing Among Private Actors. A Tale of Evolving Balances' (PhD thesis, University of Namur 2021), para 154; I Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union', (2015) 39(6) Telecommunications Policy 502-514; W Kerber, 'Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law' (2022) 67(2) The Antitrust Bulletin 280–301; See also J Zhang, 'The Paradox of Data Portability and Lock-In Effects' 2023 36(2) Harvard Journal of Law & Technology <https://ssrn.com/abstract=4728972> accessed 14 August 2024; DS Jeon, D Menicucci, 'Data Portability and Competition: Can Data Portability Increase Both Consumer Surplus and Profits?' (2024) 57 Eur J Law Econ 145–162.

[4] I Graef, M Husovec and N Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2017) Tilburg Law School Legal Studies Research Paper Series, No. 22/2017, 6–7. See also S Kuebler-Wachendorf, R Luzsa, J Kranz, S Mager,

portability diminishes the dependence of data subjects on data controllers.[5] It therefore boosts the bargaining power of data subjects,[6] also maintaining a level playing field in the digital platform economy, and heightening the quality of digital services, as well as the accuracy of data processing activities.[7] Portability can be seen as a policy lever to steward data-driven markets, by diversifying consumer choices and avoiding foreclosing practices on the side of data controllers.

It ought to be mentioned that portability existed in EU sector legislatures before the GDPR.[8] Transfers of phone numbers amongst providers in the telecommunication market have been harmonized in the Universal Service Directive (hereinafter: USD), providing "number portability" as a compulsory service for subscribers of publicly available telephone services.[9] Moreover,

---

E Syrmoudis, S Mayr, J Grossklags, 'The Right to Data Portability: Conception, Status Quo, and Future Directions' (2021) 44 Informatik Spektrum 264–272; G Lienemann, 'Global Perspectives on the Right to Personal Data Portability: Surveying Legislative Progress and Propositions for User-Led Data Transfers' (2023) SSRN <https://ssrn.com/abstract=4427736> accessed 4 June 2024; S Hondagneu-Messner, 'Data Portability: A Guide and a Roadmap' (2021), 47 Rutgers Computer & Tech LJ 240.

[5] EDPS, EDPS Recommendations on the EU's Options for Data Protection Reform [2015] OJ C 301/1, 5 (item 3.2).

[6] J Vereecken, J Werbrouck, 'Goods with Embedded Software: Consumer Protection 2.0 in Times of Digital Content?' in D Wei, JP Nehf, CL Marques (eds), *Innovation and the Transformation of Consumer Law* (Springer 2020) 94.

[7] G Nicholas, 'Taking It With You: Platform Barriers to Entry and the Limits of Data Portability' (2021) 27 Mich Tech Rev 263, 272 et seq. See also D Rubinfeld, M Gal, 'Access Barriers to Big Data' (2017) 59 Ariz L Rev 339, 364. See also L Scudiero, 'Bringing Your Data Everywhere: A Legal Reading of the Right to Portability' (2017) 3 Eur Data Prot L Rev 119; O Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017), 42(6) European Law Review 793–814; P De Hert, V Papakonstantinou, G Malgieri, L Beslay, I Sanchez, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) Computer Law & Security Review 193–203 <https://ssrn.com/abstract=3447060> accessed 12 July 2024.

[8] S Elfering, 'Unlocking the Right to Data Portability. An Analysis of the Interface with the *Sui Generis* Database Right' (2022) in *MIPLC Studies*, No. 38, Max Planck Institute for Innovation and Competition, 11; extensively M Bakhoum, B Conde Gallego, MO Mackenrodt, G Surblytė-Namavičienė, (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. MPI Studies on Intellectual Property and Competition Law, (2018) vol 28. Springer, Berlin, Heidelberg; EU Commission, *A Comprehensive Approach on Personal Data Protection in the European Union* (Communication) COM (2010) 609 final.

[9] Directive (EU) 2002/22/EC of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive) (as amended by Directive 2009/136/EC). For an overview of portability in EU sector legislation see, e.g., D Gill, J Metzger, 'Data Access through Data Portability: Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars' (2022) 8 Eur Data Prot L Rev 221.

the Payment Service Directive (hereinafter: PSD) also included a similar system to speed up payment operations. Although not explicitly referred to as portability, Articles 66 and 67 PSD establish that Member States shall guarantee the exchange of information related to individual bank accounts for payment transaction purposes.[10] Access and data transfers among providers were deemed necessary to facilitate payment operations for the ultimate benefit of consumers.

Yet, it must be noted that these Directives only contain an embryonic and sector-specific notion of portability. Therein, portability is not conceived as a prerogative that data subjects could exercise against data controllers to "reobtain" their data and switch to a new provider without losing them. Rather, portability was seen as a service that providers had to ensure, for a limited purpose, and about a specific category of data. As such, Article 30 USD established that Member States shall ensure that subscribers of publicly available telephone services are enabled to request their number to be ported. In this sense, the nature of the right differs from the GDPR portability rule. While Article 30 USD only confers a limited access right, Article 20 GDPR provides data subjects with an all-encompassing entitlement, which can be exercised in two forms: indirect and direct. The former endows the data subject with the right to receive and transfer personal data by an act of the data controller, while the latter enables direct transmission. After the transfer, the ported data will be present on both, the first and the second, except for when, according to Article 17 GDPR, the data subject decides to exercise the right to remove their data from the first data controller.

However, as portability is conditioned upon a request, it may be argued whether Article 20 GDPR also includes the right to copy personal data.[11] Undoubtedly therefore, Article 20 GDPR represents a step forward, reshaping portability as a comprehensive prerogative allowing both access to, and transfer of personal data. By contrast, its counterparts set out in USD and PSD have a much more limited scope.

As hinted at before, Article 20 GDPR prescribes for data to be transferred in a structured, commonly used, and machine-readable format. Further clarity in this respect comes from the WP29 Guidelines (WP242).[12] The Guidelines recall Recital 68 GDPR, according to which the format of data is strictly

[10] Directive (EU) 2015/2366 of 25 November 2015 on Payment Services in the Internal Market, Articles 66 and 67. Taking this legislature as a paradigm, see F Ferretti, 'A Single European Data Space and Data Act for the Digital Single Market: On Datafication and the Viability of a PSD2-like Access Regime for the Platform Economy' (2022) 14 Eur J Legal Stud 173.

[11] S Elfering (n 8), 20.

[12] Article 29 Working Party, Guidelines on the Right to 'Data Portability', adopted on 13 December 2016, as amended, and adopted on 5 April 2017, 16/EN, WP 242 rev.01 (WP29).

connected with ensuring the highest level possible of interoperability. Still, there is no duty to ensure compatibility among service providers. In general, personal data are expected to be abstractable from their format, and preference is given to open formats[13] for their capacity to further interoperability. As an example, an encrypted PDF file is not to be considered machine-readable.[14]

Portability requests are subject to several further conditions. Data must be transferred "without hindrance" for the data controller asked to meet the portability request.[15] An obstruction can occur on financial, legal or technical grounds. That means that the portability request should be technically and economically feasible for the data controller, without raising the legal basis for liability on their side against third parties. Against this ground, it can be argued that the regime set out by Article 20 GDPR still allows data transfers to a limited extent. Data controllers are not mandated to meet portability requests and may reject a request by relying on the technical or financial unfeasibility of the transfer.[16]

Moreover, data must be transferred by consent or contract, involving the data subject in the first instance. Subsequently, the transfer must take place, at least partially, through automated means, and only concern the personal data of the requesting data subject. Yet, the definition of personal data is commonly read broadly,[17] and personal and non-personal data may be so inextricably intertwined that they cannot be disaggregated, such as for bank accounts[18] under the PSD.[19] In these situations, some doubt can be cast on

[13] Ibid., 18.

[14] Ibid. See D Rubinfeld, 'Data Portability and Interoperability: An E.U.-U.S. Comparison' (2024) 57 Eur J Law Econ 163–179.

[15] Ibid., 17.

[16] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, *IPR and the Use of Open Data and Data Sharing Initiatives by Public and Private Actors*, PE 732.266, May 2022, Study Requested by the JURI Committee for the European Parliament; see also E Syrmoudis, S Mager, S Kuebler Wachendorff, P Pizzinini, J Grossklags, J Kranz, 'Data Portability between Online Services: An Empirical Analysis on the Effectiveness of Article 20 GDPR' 2021 3 Proceedings on Privacy Enhancing Technologies 351–372. See also A Diker Vanberg, MB Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8(1) European Journal of Law and Technology 1-27. Critically, J Wong, T Henderson, 'The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR' (2019) 9(3) International Data Privacy Law 173–191.

[17] N Purtova 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40–81.

[18] WP242 (n 12), 11.

[19] L Urquhart, N Sailaja, D McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2017) SSRN <https://ssrn.com/ abstract=2933448> accessed 28 July 2024, 3; P Voigt, A von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 383, 10. See G Zanfir, 'The Right to Data Portability

whether portability requests are meetable, although a relaxed interpretation of this requisite seems to be accepted by the WP29, also in line with Recital 68 GDPR.[20]

The transfer among data controllers, under an indirect data portability request, should be undertaken under EU data protection law. Nevertheless, to which extent this can occur at the expense of the receiving controller's data subjects remains to be seen.[21] Indirect portability cannot be executed, unless data protection rules protecting the receiving controller's data subjects are complied with, without going beyond the scope of the original request.[22] From this perspective, the expansive reading argued for by Drexl, under which future personal data should be held as portable, must be rejected,[23] thus limiting the scope of data transfers.

The Guidelines also shed light on the types of data that can be covered by a portability request.[24] They distinguish among provided, observed, derived, and inferred data. Provided data constitute, e.g., the infrastructure of the social network, and are directly delivered by the provider to every user, such as the Facebook homepage before registration, and the standardized format of personal accounts. Observed data reflect a higher degree of personalization, being shaped by user preferences (cookies, advertising etc.). By contrast, derived data are the byproduct of the interaction between the platform and the user, like user-generated content posted on a personal Facebook account.

Finally, inferred data are the fruit of sophisticated data processing activities performed by the data controller (e.g., profiling) resulting in customized services delivered to users. Although it may be desirable to include the more valuable observed and inferred data within the scope of the right to

---

in the Context of the EU Data Protection Reform' (2012) 2(3) International Data Privacy Law 149–162; R Janal, 'Data Portability under the GDPR: A Blueprint for Access Rights?' in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare*, (2021), Nomos, 319–342.

[20] S Elfering (n 8), 26.

[21] S Elfering (n 8), 30.

[22] This ultimately stems from the minimization principle enshrined in Article 5 GDPR.

[23] J Drexl, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC' (2018) BEUC, 110. See also H Ursic, 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control' (2018) 15 SCRIPTed 42; F Zufall, R Zingg, 'Data Portability in a Data-Driven World', in S Peng, CF Lin, T Streinz (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press 2021), 215–234.

[24] WP29 (n 12), 9 et seq.

portability,[25] WP242 has ruled it out.[26] According to Article 20 GDPR, data portability requests can only involve data "provided" by the data subject. As a result, transferred data cannot be delivered by the data controller or third parties. This condition must be read in light of the rationale underlying Article 20 GDPR.[27] Accordingly, the very same existence of data portability seeks to ensure that users become the true masters of web interactions. By this token, users should be able to "re-appropriate" uploaded content to be able to move it to a new provider. In this way, *lock-in* effects are avoided, and the diversification of digital markets is freely facilitated.[28]

Ultimately, Article 20(4) GDPR states that data processing activities undertaken by the data controller to fulfil a data portability request shall not negatively affect third parties and their prerogatives. This conflict rule principally refers to IPRs, which may have the effect of encroaching on the scope of portability. Whether or not IPRs prevail over portability is left to a fact-specific assessment, as reflected by the text of Recital 63 GDPR.[29]

III. …To Content Portability

Portability stepped outside the field of EU data protection law, also becoming a digital consumer law tool. Specifically, portability has been envisioned as a contractual remedy in the DCD, which was enacted to regulate contracts for the supply of digital content or services between users and trading

[25] W Nixdorf, 'Planting in a Walled Garden: Data Portability Policies To Inform Consumers How Much (if any) of the Harvest is Their Share' (2020) 29(135) Transnational Law & Contemporary Problems 136-165; see also P Swire, Y Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Md L Rev 335; I Graef, 'The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation' (2020) 2(2) Competition Policy International – Antitrust Chronicle 1–8.

[26] S Martinelli, 'Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"', in L Reins (ed), *Regulating New Technologies in Uncertain Times. Information Technology and Law Series*, vol 32. T.M.C Asser Press, The Hague.

[27] J Drexl et al., 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public Consultation on Building the European Data Economy' (2017) *Max Planck Institute for Innovation & Competition* Research Paper No. 17-08 <https:// ssrn.com/abstract=2959924>, accessed 9 June 2024, para 25. See also I Graef, J Verschakelen, P Valcke, 'Putting the Right to Data Portability into a Competition Law Perspective' (2023) The Journal of the Higher School of Economics, Annual Review, 53–63; J Krämer, 'Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations' (2021) 17(2) Journal of Competition Law & Economics 263–308.

[28] R Janal, 'Data Portability – A Tale of Two Concepts' (2017) 8(59) JIPITEC, para 1.

[29] S Elfering (n 8), 30.

platforms.[30] In this regard, digital platforms may be qualified as "traders" within the meaning of the DCD, if they provide users with a digital service for compensation (Recital 18 DCD).

To recalibrate the disparity in bargaining power between traders and consumers, Article 16 DCD provides the latter with a remedy against the unilateral termination of a contract. The first sentence states that "the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader". According to the second sentence, "the consumer shall be entitled to retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format".

In some respects, the conditions for submitting a portability request are stricter than those established by Article 20 GDPR.[31] The DCD portability rule is context-specific, as it can only be invoked by the user against traders with whom they concluded a contract for the supply of a digital service or content. If the trader is not the platform where the user-generated content is hosted, Article 16 DCD cannot be applied.[32] This portability right is also temporally limited as it can only be exercised in an event the contract is terminated. Termination can occur due to the lack of conformity with the contract,[33] because the relevant content or service is not received under the condition specified in the contract, and the lack of conformity is not rectified within a reasonable timeframe, free of charge and without any inconvenience for the consumer. If the defect is so gross that the counter-performance becomes disproportionate, the right to termination under Article 16 DCD can be exercised, activating the related portability right. Users may also be interested in terminating the contract in response to a trader's unilateral modification significantly affecting their interests.[34] Thus, consumers cannot always retrieve their data upon a termination. Instead, there must be some

[30] EU Directive 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, [2019] OJ L 136. See L Oprysk, 'Digital Consumer Contract Law Without Prejudice to Copyright: EU Digital Content Directive, Reasonable Consumer Expectations and Competition' 2021 70(10) GRUR International 943–956; see A Metzger et al., 'Data-Related Aspects of the Digital Content Directive', (2018) 90 JIPITEC, paras. 46–49; S Vezzoso, 'Competition Policy in Transition: Exploring Data Portability's Roles' (2021) 12(5) Journal of European Competition Law & Practice 357–369.

[31] S. Geiregat (n 1), 5 et seq.

[32] Ibid., 8.

[33] DCD, art 19(3).

[34] DCD, art 19(2).

negative and unforeseen circumstances detrimental to the point of justifying the exercise of portability rights.

Against this backdrop, portability is no longer only useful to counterbalance the weak position of data subjects in the reckless marketing of data. It rather works as a contract law remedy, allowing users to retrieve content previously uploaded on a platform that provides them with a digital service. Despite being available only under specific circumstances, i.e., when the user is unsatisfied with the non-performance of the counterparty during contract execution, this remedy goes beyond Article 20 GDPR because it is not limited to personal data "provided" by the data subject. The provisions of the DCD extend to all non-personal user-generated data uploaded by the user thanks to the service provided by the platform. It is therefore clear that also the inferred and observed data generated by the platform, based on the content previously uploaded by the user, can fall under Article 16 DCD. In this sense, the objective scope of the provision is broader than Article 20 GDPR because the DCD-remedy can be indifferently applied to all aggregated data hosted on digital trading platforms whether it is personal or non-personal.

From the GDPR to the DCD, portability changed its structure. Under the DCD, portability is not intended as a data-specific tool, applying to all content data uploaded on the trading platform. Yet contents subject to Article 16 DCD may be protected by exclusive rights, eroding the effectiveness of portability. As illustrated by Graef et al.,[35] digital content is usually made of a mixed dataset, giving rise to three different scenarios. First, IPRs can be held by data subjects, which is the ideal situation. In this case, there is no obstacle to the application of portability. The user-data subject can exercise the all-encompassing right under Article 20 GDPR to move data to a new platform, as well as the content-based rule enshrined in Article 16 DCD. Second, IPRs might however also be held by the platform, either originally or by license. In this case, it is unlikely that Article 20 GDPR applies, because it is unusual for data protected either by copyright, *sui generis* rights, or trade secrets, to be directly "provided" by the data subject. Yet, if protected data are intermingled with observed or inferred data personalizing the customer service supplied by the trading platform, the application of Article 16 DCD cannot be ruled out in an a priori manner. Third, copyright may be held by a third party, the licensing of which has not proven possible or required by the trading

[35] See I Graef (n 4), 1378; see also I Graef, T Tombal, A de Streel, 'Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer' (2019) TILEC Discussion Paper No. DP 2019-024 <https://ssrn.com/abstract=3494212>, accessed 15 August 2024. See also, in general, W Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection', (2016) 11(11) Journal of Intellectual Property Law & Practice 856–866.

platform. In that case, the balancing test of Article 20(4) GDPR is likely to be struck in favour of rightsholders, and so portability rights cannot be exercised. Instead, Article 16 DCD may still apply if, as in the case tackled before, protected and user-generated content have become so intertwined that they cannot be disaggregated. In these last two cases, it is unclear as to which extent portability can prevail over exclusive rights.

Although portability improved in scope from a data- to a content-based remedy, which can be activated by users against trading platforms, the interplay with IPRs became even more interesting. Whilst the scope of Article 16 DCD is broader than that of Article 20 GDPR, as it also includes user-generated content among the portable data category, the risk of conflict with IPRs has increased. Furthermore, if Article 20(4) GDPR clarifies that the relationship with IPRs is left to a case-by-case balancing test, Article 16 DCD stays silent in this respect, leaving room for its under-implementation due to IPRs.

IV. …To Cross-Border Content Portability

The previous two sections (II and III) illustrated the multifaceted role of portability in EU law has. Yet, despite the differences in scope and function between Articles 20 GDPR and 16 DCD, it was noted that IPRs indifferently constitute a relevant obstacle to the applicability of both portability provisions. As personal data are difficult to disaggregate from non-personal content data, whether portability can operate and serve its purpose is uncertain. It was also stressed that the role of portability changed, moving from the data law field to becoming a content regulation tool, backed by the aim of empowering consumers against platforms. In the years afterwards, portability became a feature of online content, useful to guarantee a higher circulation of content across the EU. This is the rationale behind the Portability Regulation, the first attempt to regulate the intricate interface between IP law and content portability. In the context of this Regulation, content portability plays a key role in balancing the interests of copyright holders against those of users, being useful to ensure cross-border access to content.[36]

Article 3 PR imposes a portability duty on providers of "online content services", encompassing every type of linear and non-linear provision of audiovisual, visual or audio content. The ample notion includes music streaming

[36] Regulation (EU) 2017/1128 of the European Parliament and the Council of 14 June 2017 on Cross-Border Portability of Online Content Services in the Internal Market [2018] OJ L 168/1. See also S Engels, JB Nordemann, 'The Portability Regulation (Regulation (EU) 2017/1128): A Commentary on the Scope and Application' (2018) 9 JIPITEC 179, para 1.

services such as Spotify, online game marketplaces, and on-demand video-sharing platforms like Netflix, Vimeo and Amazon Prime. The beneficiaries of portability are subscribers of online content services, technically defined as consumers who, in virtue of a contract for the supply of an online content service for a fee or free of charge, are entitled to access such service in the Member State of their residence. In this sense, the legal relationship is the same as between traders and users under the DCD.

Importantly, the meaning of "portable" in the Portability Regulation is spelt out peculiarly. In contrast with the aforementioned EU legislation addressing portability, Article 2 PR defines it as "a feature of an online content service whereby subscribers can effectively access and use the online content service in their Member State of residence without being limited to a specific location."[37] Portability has thus become an inner characteristic of online content not uploaded by the users but offered by the provider for a fee. Cross-border portability is not a legal prerogative of subscribers, but an essential feature of online content services supplied by contract. It amounts to an obligation placed on providers and, at the same time, a quality standard requirement for online content.

Article 3 PR imposes the cross-border portability of subscription services for subscribers who are temporarily present in a Member State other than the one of residence. The broad scope of the provision can be inferred from two aspects. First, the notion of "paid subscribed service" includes both direct and indirect forms of payment of the provider. This confirms that portability here is not conceived as a contract law remedy to be asserted by subscribers against digital platforms with a view to avoiding *lock-ins* or abuses of bargaining power. Rather, it is conceived as a compulsory quality standard for online content. Second, the notion of "temporary residence" establishes a legal fiction, under which subscribers should be treated as if they were still located in the Member State of residence even during a stay in another MS.

In this way, providers do not have clear exploitation rights in all Member States thanks to an equivalence rule, allowing subscribers to access content while travelling across the EU, as if they never moved. However, the criteria to determine when a subscriber is "temporarily present" in a Member State, and the maximum time limit, are clouded in uncertainty. In contrast with Articles 20 GDPR and 16 DCD, Article 3 PR is content-specific and operates despite IPRs. As noted in the first lines of this section, the PR is the first piece of EU law where the balance between IPRs and portability is struck within the very text of the portability provision. Article 3 PR overcomes the fact that online content is protected by IPRs, setting a portability rule for the very purpose of avoiding

[37] Ibid., 185.

clashes with exploitation rights. Portability operates to prevent abuses in the enforcement of IPRs, which may lead to unfair restrictions and undermine the quality of services offered by online content providers.

The Portability Regulation also contains safeguards against circumvention practices, which may be undertaken by restricting the functionalities of a given service while abroad. Subject to an equivalence rule, providers are compelled to provide subscribers with the same content, devices and functionalities in the Member State of residence and in the country of temporary stay. Yet, it is not clear whether this "quality requirement" amounts to a binding duty to refrain from setting access restrictions based on the quality of the services provided on a cross-border level.[38]

The said Regulation does not provide any EU-wide harmonized enforcement system for claims based on the lack of compliance with Article 3 PR. In this regard, Article 7 PR only states that every clause contrary to the portability rule shall be unenforceable. As highlighted in a later study,[39] the application of Articles 3 and 7 PR resulted in an adjustment in licensing practices. Most agreements concluded between providers and rightsholders after the Regulation incorporate the portability duty.[40] In this respect, it is also worth noting that Article 7 PR applies horizontally, i.e., regardless of the contract law regulating the license between the provider and rightsholders, as well as the subscription contract between the provider and its subscribers.

There is also mutual reinforcement between the portability rule enshrined in Article 3 PR, and the remedy envisaged in Article 16 DCD. If providers do not implement cross-border portability in line with Article 3 PR, this non-compliant behaviour can amount to a lack of conformity within the meaning of Article 16 DCD, allowing subscribers to activate available remedies in the form of the termination of the contract, or to have it brought to conformity with, previously absent, cross-border portability. Being identified as one of the requirements of objective conformity,[41] it is clear that portability has become an essential feature of online content, despite the applicable contract law and the subsistence of valid and enforceable IPRs. Against this background,

[38] Ibid., 187.

[39] Study for the EU Commission, Visionary Analytics, *Study on the Portability Regulation*, (2022) 104.

[40] Ibid., 43–44.

[41] Ibid. See also See also KW Lindroos, NHB Hang, 'The Portability Regulation' in I Stamatoudi, P Torremans, (eds), *EU Copyright Law,* 2nd ed, 575–609; G Mazziotti, 'Allowing Online Content to Cross Borders: Is Europe Really Paving the Way to a Digital Single Market?' in Pihlajarinne, T, Vesala J, Honkkila, O (eds), *Online Distribution of Content in the EU*, (2019) Edward Elgar Publishing 188–203; TE Synodinou, 'The Portability of Copyright-Protected Works in the EU' in TE Synodinou, P Jougleux, C Markou, T Prastitou, (eds) *EU Internet Law* (2017) Springer 217–266.

providers are incentivized to implement this requirement extensively, also to avoid consequences such as contract termination.

Thus, the Portability Regulation has been paramount in expanding access to prerogatives granted to subscribers of online content at the expense of copyright exclusivity. The portability obligation enshrined in Article 3 PR helps with discouraging the artificial extension of exclusionary prerogatives beyond territoriality, providing a quality and minimum access standard for online content. Recital 10 PR makes explicit that the Regulation seeks to abolish unrestricted geo-blocking measures. Thanks to Articles 3 and 7 PR, contract terms or technical measures including geo-blocking, which can prevent access to online content services, are treated as unenforceable, creating a barrier to the expansion of IPRs. In this respect, the policy purpose behind the PR goes hand in hand with that of the Geo-Blocking Regulation (hereinafter: GR), enacted in the same year in order to prevent discrimination among customers given their country of residence or nationality. Yet, Article 1(5) GR states that the provisions thereof apply without prejudice to the rules of copyright and neighbouring rights, and, in the same fashion, Article 1(3) GR explicitly excludes audiovisual services from its scope. By way of contrast, the PR does not exclude copyrighted content from its field of application. Rather, Article 3 PR derogates from IP exclusivity to guarantee cross-border portability.

V. The Digital Markets Act (DMA): Bridging the Gap between Content Portability and Access to Data

The Digital Markets Act[42] evaluates the role of portability as a quality standard for online content. The Regulation targets "gatekeepers", identified

[42] Regulation (EU) 2022/1925 of the European Parliament and the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), [2022] OJ L 265/1. For further commentary, see A De Streel, P Alexiadis, 'The EU's Digital Markets Act: Opportunities and Challenges Ahead' (2022) 23(2) Business Law International 163–201; P Akman, 'Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act', (2022) European Law Review 47, 85 <https://ssrn.com/abstract=3978625>, accessed 3 June 2024; C Cennamo, T Kretschmer, P Constantinides, C Alaimo, J Santaló, 'Digital Platforms Regulation: An Innovation-Centric View of the EU's Digital Markets Act', Journal of European Competition Law & Practice, January 2023, Vol 14, Iss 1, 44–51; P Bongartz, S Langenstein, R Podszun, 'The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers', Journal of European Consumer and Market Law, (2021), Vol 10, Iss 2, 60–67; N Moreno Belloso, N Petit, 'The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove' European Law Review (2023), 48, 391, available at SSRN: <https://ssrn.com/abstract=4411743>, accessed 24 May 2024. On the evolution of portability see B Lazarotto, 'The Right to Data Portability: A Holistic Analysis

in Article 3 DMA in the light of their significant impact on the market, enjoying a strong, entrenched and durable market position, being the providers of a core platform service, which behaves as a gateway for business-users to reach end-users. Portability is included among the obligations pending upon gatekeepers under Article 6 DMA. Specifically, this provision includes several duties that directly and indirectly aim to guarantee an adequate level of portability and interoperability. Aligning with the rationale underlying Article 3 PR, Article 6(6) DMA specifies that the gatekeeper "shall not restrict technically or otherwise the ability of end users to switch between and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper, including as regards the choice of Internet access services for end users." Along the same lines, Article 6(7) DMA provides that the gatekeeper shall ensure access to and "effective interoperability" among operating systems, hardware and software features, as well as implementing safeguards to avoid compromising their integrity.

One of the main rationales of portability is to ensure interoperability in digital markets. Yet none of the aforementioned provisions sets a mandatory obligation to ensure compatibility among hardware and software applications. This issue appears for the first time in the EU in the DMA. Gatekeepers are subject to an interoperability duty for the benefit of businesses and end-users under Article 6(6) DMA, preventing restrictions to switching. Interoperability and portability from a technical and legal point of view are firstly spelt out as two sides of the same coin.

The two most relevant portability provisions are infused within the texts of Articles 6(9) and 6(10) DMA. The former resembles Article 20 GDPR, by allowing end users, and third parties authorized by them, to "port" data provided by, or generated through the use of the core platform service. According to Article 6(9) DMA, gatekeepers must provide users with "continuous and real-time access to data." Article 6(10) DMA envisages the same rule for business users and third parties acting on their behalf, also specifying that access to aggregated and non-aggregated data is limited to personal data generated through the use of the services provided by business users, and to the extent sharing is permitted by consent.

---

of GDPR, DMA and the Data Act', EJLT, (2024), Vol 15, n 1, 1–15. On the regulatory role of portability see also M Borghi, 'Data Portability and Regulation of Digital Markets', CIPPM / Jean Monnet Working Papers, (September 2019), Bournemouth University, available at SSRN: <https://ssrn.com/abstract=3617792>, accessed 15 May 2024. On the relationship between the DMA and the GDPR see D Geradin, K Bania, T Karanikioti, 'The Interplay between the Digital Markets Act and the General Data Protection Regulation' (29 August 2022), <https://papers.ssrn.com/abstract=4203907>, accessed 30 June 2024.

The DMA envisages portability as an expanded access right modelled on Article 15 GDPR. This view of portability dates back to the draft version of Article 20 GDPR, as the Commission previously planned to incorporate the two rights in a catch-all access prerogative.[43] The DMA provisions go significantly beyond the sector- and data-specific approaches found in the GDPR, the DCD and the PR. The DMA text does not distinguish according to the type of data, allowing portability to the extent the same has been "provided" and generated by users. Moreover, Articles 6(9) and 6(10) DMA operate on a time-shifting basis, in a way that gatekeepers are mandated to ensure continuous and real-time access to data. This provides users with substantial control over such data. Despite being broader in scope than the aforementioned provisions, DMA provisions on portability go back to the original rationale of portability. Rather than being conceived as an essential feature of online content, like in the PR, portability within the DMA returns to being a legal tool allowing users to access data. Although such prerogative is not directly attributed to the data subject, gatekeepers must ensure it through compliance with the related obligation.

Yet, the interface between the access/portability rules and IPRs is not clarified in any part of the DMA. Like the DCD, the DMA does not contain a word in this regard. As in the case of Article 3 PR, lack of compliance with the obligations embedded in Articles 6(9) and 6(10) DMA, can amount to non-conformity, triggering the application of Article 16 DCD, and thus leading to the termination of many digital contracts. As portability duties have an impact on the execution of digital contracts for the supply of core platform services, gatekeepers are highly pressured to comply with portability duties and to ensure access to portable data. In this light, compliance with Articles 6(9) and 6(10) DMA is fundamental to avoid the termination of digital contracts with business users, and thus revenue sources for the gatekeepers themselves. In this vein, Recital 63 DMA prohibits undermining the right of users to subscribe to a new core platform service by making them pay additional fees for doing so, or by making the act of switching more difficult on a contractual or technical level.

[43] S Elfering (n 8), 19 et seq. See also European Parliament, 'Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)' A7-0402/2013, amendment 111. On EU data access provisions introduced with the DMA see, e.g., PG Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, Further EU Digital Regulation Acts, and Competition Law' (2023) 14(2) Journal of European Competition Law & Practice 67–82; P Baschenhof, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?' U Ill JL Tech & Pol'y (2022) 1; C Etteldorf, 'DMA – Digital Markets Act or Data Markets Act?' (2022) 8 Eur Data Prot L Rev 255.

VI. Article 17 of the Copyright Digital Single Market Directive (CDSMD): The Impact of Content Filtering on Portability

Today, copyright enforcement and digital platform regulation are indissolubly intersected.[44] As observed before, portability rights are usually exercised by users against digital platforms, which may hold IPRs themselves over the retrievable or portable stock of data. Where IPRs are held by third parties, digital platforms are incentivized to monitor content uploaded by users to avoid allegations of contributory infringement.[45]

It has been noted that several provisions go in the direction of bolstering interoperability in the digital ecosystem, thanks to remedies inspired by a portability logic in the EU. However, the pro-competitive rationale of these legal tools is at risk if the digital platform finds itself in danger of being held liable for complying with portability duties. The position of the data controller can be attributed to an aggregating platform that hosts, indexes, and makes digital content available to users. Content can be either user-generated or provided by the platform itself. Content forms datasets can be protected either

[44] Legal literature on the matter is enormous. Just to mention a few, A Metzger, M Senftleben, 'Understanding Article 17 of the EU Directive on Copyright in the Digital Single Market – Central Features of the New Regulatory Approach to Online Content-Sharing Platforms', Journal of the Copyright Society of the U.S.A. 67 (2020), 279 (284–308); C Geiger, BJ Jütte, 'Platform liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match', Gewerblicher Rechtsschutz und Urheberrecht International (2021), 70, 517; SF Schwemer, 'Article 17 at the Intersection of EU Copyright Law and Platform Regulation', Nordic Intellectual Property Law Review (2020), 400–435; M Senftleben, 'Institutionalized Algorithmic Enforcement – The Pros and Cons of the EU Approach to Online Platform Liability', Florida International University Law Review (2020), 14, 299–328; M Husovec, JP Quintais, 'How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive', Gewerblicher Rechtsschutz und Urheberrecht International, (2021), 70, 325–348; JP Quintais, G Frosio, et al., 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics', JIPITEC (2020), 10, 277–282; G Frosio, 'Reforming the C-DSM Reform: A User-Based Copyright Theory for Commonplace Creativity', IIC (2020), 51, 709; M Senftleben, 'Bermuda Triangle: Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market', EIPR, 2019, 41, 480; M Senftleben, C Angelopoulos, et al., 'The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform', EIPR, (2018), 40, 149; G Frosio, 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe', Oxford Journal of Intellectual Property and Practice, (2017), 12, 565–575; G Frosio, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy', Northwestern University Law Review, (2017), 112, 19.

[45] Extensively, J Riordan, 'A Theoretical Taxonomy of Intermediary Liability' in G Frosio (ed), *The Oxford Handbook of Online Intermediary Liability*, (2020) Oxford University Press, 78.

sui generis, or by copyright held by the platform, or third parties.[46] At the same time, protected content may be retrievable under Article 16 DCD, upon termination of the contract between the trading platform and the user for the supply of a digital service or content.

Part of the data provided by the user can be included in a portability request, to be addressed by the data controller-aggregator under Article 20 GDPR. Sometimes, the aggregator is also eligible in its position of a "provider of online content services", within the meaning of Article 2 PR, being subject to the cross-border portability rule enshrined in Article 3 PR. Content provided under the subscription contract is, therefore, mandatorily "portable" and accessible to subscribers also when temporarily present in a Member State other than the country of residence. Moreover, if the aggregator is a "gatekeeper", the same is also subject to the obligations mandated by Article 6 DMA, including the duty of ensuring continuous and real-time access to the data provided, or generated through the use of the core platform service.

As a result, a digital platform can be subject to several portability obligations, due to its multiple roles as a "trader" of a digital service or content, a "data controller", "provider of online content services", and a "gatekeeper". The same entity can own, or license exclusive rights over some, or all content made available, also being the licensee thereof. In this case, these IPRs may prevent access to portable content or data.

Yet the relationship between IPR enforcement and portability remained mostly unaddressed. It is unclear whether the remedies set by Article 16 DCD can be applied to content provided by users, notwithstanding the subsistence of IPRs entitled to third parties. Providing little help in this regard, Article 20(4) GDPR also refers to the need to strike a balance to determine whether a portability request can be refused on the grounds of IP law. Likewise, the DMA does not shed light on whether Articles 6(9) and 6(10) DMA can apply when content to be made accessible is covered by IPRs. The same conundrum thwarts the applicability of Article 3 PR, because the notion of "temporary residence" remains undefined. Therefore, the provision contains an exception to copyright territoriality, which risks being extended at the expense of copyright holders.

As a consequence, how much digital platforms are likely to comply with portability obligations mostly depends on to what an extent IPRs are enforceable. This, in turn, may be affected by the infringement liability regime set for digital platforms. In all the cases explained above, the main issue rests on whether protected content can be held portable. In this regard, Article 17 CDSMD establishes an articulated copyright enforcement system, which risks

[46] J Drexl (n 27), 77.

incentivizing platforms to filter or block (protected) content *ex-ante*, with the effect of hampering portability.

Article 17 CDSMD targets a sub-type of content providers, which may overlap with the definition of "gatekeepers" under the DMA, as well as with that of "online content service providers" of Article 2 PR. In this sense, the provision applies to "online content-sharing service providers" (hereinafter: OCSSPs), identified in Article 2(6), para 1 CDSMD with "providers of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject-matter uploaded by its users, which they organize and promote for profit-making purposes". Whether a digital platform falls under this definition must be assessed case-by-case, relying on "a combination of elements, such as the audience of the service and the number of files of copyright-protected content uploaded by the users of the service". To fit in the definition, the service provided by the platform should have a profit-making character,[47] taking inspiration from the "diligent economic operator" benchmark set out in the Court of Justice of the European Union (hereinafter: CJEU) case law.[48] In addition, the act of making content available should be the main activity undertaken by the provider, as well as the main source of its income.

Article 17 CDSMD relies on a two-tiered liability regime. The content provider can be held directly liable for performing unauthorized acts of communication to the public of protected content. Then, OCSSPs can also be found secondarily liable for the infringing acts performed by users who upload protected content without authorization. This direct liability regime is set by Article 17(1) CDSMD. Whether online content-sharing service providers can be held liable under this provision may depend on the reading of the concept of "communication to the public" enshrined in Article 3(1) of the Information Society Directive (hereinafter: InfoSocD).[49]

According to the latest interpretation of the CJEU, to find an infringement of Article 3(1) InfoSocD the following elements must be present: the existence of an act of communication of a protected work, and the direction of the

[47] *L'Oréal SA and Others v eBay International AG and Others*, C-324/09, ECLI:EU:C:2011:474 paras. 89 et seq.

[48] For further commentary, SF Schwemer, (n 45), 410 et seq.

[49] Article 3(1) InfoSoc transposes Rome Convention (International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations), adopted in 1961 and entered into force in 1964, Article 3, para (d). See also G Frosio, 'It's All Linked: How Communication to the Public Affects Internet Architecture' (2022) Computer Law & Security Review 37.

same to the public, requiring an individual assessment for both.[50] Given the indispensable role of OCSSPs in providing users with a high number of content, the Court clarified that users must be held responsible for their own choices.[51] Consequently, OCSSPs perform an act of communication to the public, for which they can be held liable under Article 17(1) CDSMD, only when they act in "full knowledge" of the infringing nature of the content made available, that means if their act is "deliberate".[52] With this judgment, the CJEU increased the threshold to hold providers liable for contributory infringement, also reducing the scope of Article 17(1) CDSMD.

Nevertheless, it can be argued whether the direct liability standard of Article 17(1) CDSMD relies on the notion of communication to the public developed in CJEU case law or, alternatively, if a new concept has been implicitly introduced under the CDSMD. If the first interpretation is correct, a knowledge requirement enters the assessment to find liability under Article 17(1) CDSMD. In the latter case, Article 17 CDSMD gives rise to a new notion of communication to the public, defined by the conduct undertaken by OCSSPs, excluding subjective factors. Therefore, the strict liability rule of Article 17(1) CDSMD is likely to produce a hyper-deterrent effect, due to the uncertainty surrounding the notion of "communication to the public", with the risk of disincentivizing the making of a high number of content available to users.

Several portability rules have been enacted in the form of obligations to be addressed by online content-sharing service providers, requiring "deliberate" acts of making "portable" content available to the public. By complying with the portability obligations of Articles 6(9) and 6(10) DMA, OCSSPs are likely to perform an act of communication to the public. This opens the door to liability under Article 17(1) CDSMD if the content that should be made accessible to end-users are covered by IPRs held by other business users, the gatekeeper itself, or third parties. Likewise, when providers are compelled to return content to users under Article 16 DCD, the content at stake might be indissolubly intermingled with protected ones, forming mixed datasets that can be difficulty disaggregated.

A similar situation can also stem from an extensive reading of Article 3 PR. In compliance with this rule, providers of online content services are required to ensure cross-border access to copyrighted content, without clearing exploitation rights in each Member State of a temporary residence. If the concept of "temporary residence" is interpreted broadly, providers risk

[50] *Frank Peterson v Google LLC and Others and Elsevier Inc.v Cyando AG*, C-682/18 and C-683/18, ECLI:EU:C:2021:503.

[51] Ibid., para 71.

[52] Ibid., para 80.

performing unauthorized acts of a communication to the public. Undertaken in order to execute portability obligations, the act of making protected content available is likely to be the "deliberate" outcome of a balancing act. Providers risk finding themselves at a crossroad – they must avoid infringements of IPRs while, at the same time, ensuring portability. The outcome of this balancing act is left to providers on a case-by-case basis, leading to uncertainty as to both the scope of IP enforcement and the level of compliance expected with respect to portability obligations.

The interplay between portability and liability for copyright infringement becomes more contrived under Article 17(3) CDSMD. According to this provision, online content-sharing service providers can be held secondarily liable for unlawful acts of communication to the public performed by users. Nevertheless secondary liability can be avoided if the cumulative conditions enlisted in Article 17(4) CDSMD are fulfilled. Firstly, OCSSPs must primarily prove to have made "best efforts" to obtain authorization from copyright holders and conclude the highest number possible of licensing agreements to avoid uploads that infringe IPRs. Secondly, they need to demonstrate that they have made unavailable to the public content for which the rightsholders provided the OCSSPs with all relevant and necessary information. Thirdly, once notified, OCSSPs must prove to have acted expeditiously to remove infringing content and prevent its future unauthorized uploads upon notice.

This provision also contains a grey list of uploaded content submitted to a notice and a stay-down regime,[53] i.e., to be removed upon a sufficiently substantiated notice. Article 17(4) CDSMD draws particular attention to a specific category of relevant content (such as a pre-released song or podcast on Spotify). Not-removed content that belongs to this list gives rise to liability. The making available of such content is the self-evident proof that the OCSSP has not made sufficient efforts to avoid the uploading of infringing content, being unable to satisfy the conditions under Article 17(4) CDSM. Against this background, secondary liability may not only arise when providers have not expeditiously reacted to a notice sent by copyright holders, but also for not having undertaken the "best efforts" to prevent future uploads, and the reappearance of infringing content online.

The Pandora Box of Article 17(4) CDSMD rests on the concept of "best efforts". This standard can incentivize "anti-portability practices", undertaken by online content-sharing service providers to escape liability under Article 17(3) CDSMD. Abstractly, OCSSPs must conclude the highest number possible of licensing agreements to ensure that content is uploaded

[53] A Kuczerawy, 'From 'Notice and Takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression' in G Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020), 525–543.

and made available with authorization. Yet, identifying rightsholders is often practically impossible and disproportionately burdensome for OCSSPs. As a result, providers may be tempted to resort to Article 17(4)(b) CDSMD to avoid secondary liability. Accordingly, they need to demonstrate to have "made, by high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided the service providers with the relevant and necessary information".

The standard of "best efforts" is highly uncertain, as Article 17(4) CDSMD does not provide any useful guideline about which industry standards of professional diligence should be followed. In this respect, the current text of the provision risks encouraging preventive blocking or filtering practices.[54] It is worth noting that the Polish Government filed an unsuccessful complaint to the CJEU to obtain a revision, claiming that the current configuration of Article 17(4) inevitably leads to infringements of freedom of expression under Article 11 CFREU. It was pointed out that the wording of the provision is likely to induce over-filtering and over-blocking as OCSSPs strive to comply with the best efforts requirement.[55] Even the Guidance issued by the Commission did not add much clarity in this respect, although it was meant to cast light on whether the best efforts standard implies the adoption of blocking and filtering technologies *ex-ante*.[56] The Guidance only recommends a bifurcated solution: one, filtering "manifestly infringing" content *ex-ante*;[57] and two, in other cases, rightsholders are required to provide all relevant and necessary information concerning the infringing character of content through "earmarking".[58] In this latter situation, online content-sharing service providers can also submit the earmarked content to human review before deciding to block or filter it. Yet, this human review recommended by the Commission should have extraordinary capacities, considering that, at present, automated filters are not even capable of

---

[54] C Geiger, BJ Jütte, 'Towards a Virtuous Legal Framework for Content Moderation by Digital Platforms in the EU? The Commission's Guidance on Article 17 CDSM Directive in the light of the *YouTube/Cyando* judgement and the AG's Opinion in C-401/19', EIPR (2021), 43:10, 625–635.

[55] *Republic of Poland v European Parliament and Council of the European Union*, C-401/19, ECLI:EU:C:2022:297, 5 et seq.

[56] EU Commission Communication, *Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market* COM/2021/288 final, commented by JP Quintais, 'Commission's Guidance on Art. 17 CDSM Directive: the authorization dimension', posted on *Kluwer Copyright Blog* on 10 July 2021; G Priora, BJ Jütte, 'A Further Step into a Systematic Distortion: The EC Guidance on Article 17 CDSM Directive Further Complicates Copyright Exceptions', posted therein on 9 June 2021.

[57] COM(2021) 288 final, 13.

[58] Ibid., 22.

distinguishing lawful uses from infringing ones.[59] In this sense, the Commission prophesized the language later deployed by the CJEU while addressing the Polish claim.[60] The Guidance upheld *ex-ante* filtering and blocking measures of manifestly infringing content, also providing a non-exhaustive list of examples.[61] In these situations, the OCSSP is not even required to make an independent assessment concerning the legality of the upload and can immediately filter it.[62] Hence, *ex-ante* filtering and blocking without prior assessment is permitted, and even recommended, regardless of the high risk of unfounded notices.

The act of earmarking content risks overthrowing the two-tiered liability framework of Article 17 CDSMD into a direct liability one. This may lead to the proliferation of filtering and blocking practices *ex-ante,* in the attempt to escape from an unclear liability threshold. In the words of the Commission, the act of making manifestly infringing or previously earmarked content available amounts to an act of communication to the public performed by the OCSSP, triggering direct liability under Article 17(1) CDSMD.[63] In this regard the already mentioned lack of coordination between the CJEU reading of Article 3(1) InfoSoc and the strict liability standard of Article 17 CDSMD, increases uncertainty as to when OCSSPs should be held liable for performing an unauthorized act of communication to the public.[64] From this perspective, the suggestions of the Commission as to how to comply with the best effort requirement might produce a conflation between the primary and the secondary liability standards of Article 17(1) and (3) CDSMD, exacerbated by the lack of clarity over the notion of "communication to the public".

In this scenario, online content-sharing service providers can be held primarily liable for deliberately communicating protected content to the public in order to ensure portability, and secondarily liable for not having undertaken the "best efforts" to prevent the uploading of unauthorized content through filtering and blocking technologies. According to the Commission, to align with the best effort requirement, OCSSPs are therefore compelled to undertake a specific conduct, but for being held secondarily liable for having acted in full knowledge of the infringing character of the content. The necessity of preventing uploads of manifestly infringing and earmarked content increases the threshold to prove compliance with the best efforts-requirement. In this

[59] C Geiger, BJ Jütte (n 54), 12 et seq. See also J Reda, J Selinger, M Servatius, *Article 17 of the Directive on Copyright in the Digital Single Market: A Fundamental Rights Assessment* (Study for Gesellschaft für Freiheitsrechte), (December 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3732223>, accessed 10 March 2024.

[60] *Republic of Poland v European Parliament and Council of the European Union* (n 55), 12.

[61] COM (2021) 288 final, 21.

[62] C Geiger, BJ Jütte (n 54), 10.

[63] *Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG* (n 50), para 94.

[64] Ibid., paras 84–100.

sense, the adoption of filtering and blocking measures *ex-ante* is likely to become the safest shortcut to avoid liability.

Briefly, the concept of "best efforts" is likely to be interpreted as a high standard mandating the implementation of preventive blocking and filtering of content, which may be held "portable", with the ultimate effect of hindering the effectiveness of portability rules. In this sense, the regime set out in Article 17 CDSMD exacerbates the lack of coordination and increases the difficulties in reconciling the scope of the various portability rules. To make an example in this regard, the situation of business users holding IPRs over content uploaded on platforms operated by gatekeepers can be considered. These can "earmark" such content also upon an unfounded notice, encroaching on the scope of portability obligations embodied in Articles 6(9) and 6(10) DMA at the expense of users. This may ultimately lead to the under-implementation of the portability obligations included in the DMA and, in turn, to a conflict of interests between end-users, entitled to real-time and continuous access to data generated through the use of core platform services, and business users, who have the same prerogative coupled with that of exercising exclusive rights over the protected content generated through the use of such services. This creates an unfair disparity between end-users and business-users, which hampers the ultimate goal of portability, guaranteeing a higher diversification of digital services and markets.

If the content uploaded by business users have become inextricably intermingled with other protected content, later earmarked and filtered, the aggregated content may become no longer accessible, notwithstanding the applicability of Article 6(9) DMA. Yet, the very same inapplicability of Articles 6(9) and (10) DMA can amount to objective non-conformity of the digital service supplied by contract, triggering the remedies enshrined in Article 16 DCD and ultimately leading to contract termination. Termination of a high number of contracts may have disruptive effects on gatekeeper platforms with destabilizing effects on the market. Hence, to reconcile the objective of the two rules (Article 6 DMA and Article 16 DCD), the extensive implementation of *ex-ante* blocking and filtering systems is likely to result in a reduction in the scope and effectiveness of Article 16 DCD. If business users generate protected content by using a core platform service provided via an OCSSP gatekeeper, end-users are unlikely to visualize it, as such content might be intermingled with protected content, earmarked and filtered *ex-ante*. Instead, the interface between the incentive to filter, stemming from a systematic interpretation of Article 17 CDSMD and Articles 6(9) and 6(10) DMA remains unaddressed. Its implications on the digital ecosystem are therefore not easily predictable.

In the same fashion, providers of online content services may be incentivized to under-implement Articles 3 and 4 PR for fear of liability under Article 17 CDSMD. In fact, as the notion of "temporary residence" is undetermined, OCSSPs providing online content services within the meaning of Article 2 PR might be surreptitiously pushed to narrow down the scope of the portability duty through the implementation of filtering technologies with the effect of reducing cross-border access at the expense of subscribers. As seen above in the case of DMA provisions, also the lack of compliance with Articles 3 and 4 PR can amount to non-conformity of the service offered through the subscription contract, potentially leading to its termination.

Ultimately, as already noted, Article 20(4) GDPR does not prescribe a specific outcome for the balancing test that data controllers are required to perform to reconcile the subsistence of IPRs with the effectiveness of portability rights. Thus, if the personal data subject of a portability request issued by a user of an online content-sharing service has later become intersected with protected content of third parties, OCSSPs are likely to outright refuse the portability request to avoid liability under Article 17 CDSMD. Against this background, online content-sharing service providers are eager to resort to the shortcut of refusal rather than disaggregating data for fear of the low liability threshold set by the provision.

VII. Concluding Remarks

This paper aimed to investigate the multifaceted and evolving role of portability in the digital arena, shedding light on its interplay with IPRs enforcement. First were discussed the prerogatives conferred by Article 20 GDPR to data subjects to transfer their personal data to a new provider (**II**), focusing on the ambiguities and differences of the portability provisions first appeared in specific sectors of EU law. It was pointed out that the applicability of Article 20 GDPR is conditional upon several factors, as well as limited to specific categories of personal data. In addition, IPRs are also able to preclude such applicability.

Afterwards, Article 16 DCD was tackled, highlighting its divergences from Article 20 GDPR (**III**). Despite being context-specific, it was observed that this provision contains a portability remedy for digital users *vis-à-vis* trading platforms, also extending to non-personal data. Yet it was noted that the same does not address the interplay with IPRs. This creates uncertainty as to whether Article 16 DCD may apply to mixed datasets. In this sense, the relationship with IPRs remains complicated.

In any case, it was highlighted that Article 16 DCD reflects an evolved concept of portability, which has become a consumer law remedy, acting as an objective conformity standard for a category of digital contracts. Portability is therefore no longer merely a prerogative of data subjects operating with sole regard to their personal data, but also extending to cover data generated through the use of a digital service supplied by contract.

Under the Portability Regulation, portability was designed as an essential feature of online content services (**IV**). Going further than the aforementioned provisions, Article 3 PR sets out a legal fiction to avoid clearance of exploitation rights across the EU. In contrast with Articles 20 GDPR and 16 DCD, portability prevails here over IPRs under specific circumstances, deviating from the principle of copyright territoriality. Article 3 PR sets a prevalence rule to avoid clashes between portability and copyright, allowing subscribers to access online content when temporarily present in a Member State other than the one of residence.

Despite its flaws, the Portability Regulation has the merit of conceiving portability as a content regulation tool, useful to limit the artificial expansion of the scope of IPRs. It can be reasserted that after the enactment of the PR, licensing agreements for online content started including portability as a standard requirement. Non-compliance with Article 3 PR could, therefore, amount to objective non-conformity of the digital contract, leading to its termination. From this overview, it was preliminarily inferred that the various remedies in EU law inspired by the portability logic are mutually enforceable and tend to progressively erode the contours of IPRs. If, on one hand, the proliferation of many different concepts of portability increased uncertainty, then, on the other hand, portability started playing multiple roles, touching upon multiple areas of EU law and impacting on digital platform regulation.

Portability can be indifferently conceived as a standard requirement for online content (Article 3 PR), a consumer law remedy against abuses of bargaining power (Article 16 DCD), and a prerogative of data subjects to transfer their data from one data controller to a new one (Article 20 GDPR). Completing this patchwork of definitions and remedies, Articles 6(9) and 6(10) DMA were analysed (**V**). These two provisions contain portability obligations that must be implemented by digital gatekeepers to confer access rights to data generated using the core platform service for the benefit of users. The attention was specifically drawn to convergences and intersections with other portability rules.

After delving into the bewildering scenario of EU portability law, it was concluded that one of the most problematic issues damaging its applicability is the unclear relationship between the scope of portability rights and IPRs. In this sense, Article 3 PR is an isolated case in that it pre-determines that

relationship, operating, however, under very specific circumstances. Other relevant provisions, such as Articles 6(9) DMA and 6(10) DMA, fail to explicitly address the problem. There is some risk of a situation arising where the broader the scope of data portability rights, the lesser the probability of giving them full effect will be because of the existence of IPRs. Thus, IPRs can hinder the effectiveness of portability provisions, hampering their coordination, and even further encroaching on their scope, which is usually read in a restrictive manner. This underpins the role of portability as a content-regulating tool as well as a pro-competitive instrument. To understand whether IPRs enforcement can be a relevant obstacle to portability, especially when its implementation is left to digital platforms, Article 17 CDMSD was explored in depth, investigating its contradictions and influence on EU data-driven platform regulation (**VI**).

In particular, the last section of this paper shed light on the complexities of the two-tiered content providers' liability system for copyright infringements as set out in the text of the provision, stressing the interpretative doubts looming in the background. It was pointed out that such ambiguities may give rise to hyper-deterrence and lower the liability threshold. In turn, hyper-deterrence can push digital gatekeepers to under-implement portability obligations, in order to escape from copyright infringement liability and comply with the best-effort requirement. Hence, gatekeepers are incentivized to implement large-scale filtering and blocking technologies in order to avoid secondary liability for copyright infringement, with the effect of reducing the number of accessible and portable content. As a result, the applicability of many portability provisions can be excluded, or their scope reduced to the minimum.

To sum up, despite the growing role of portability as a digital content regulating tool functional to maintain an adequate level of competition in data-driven markets, its scope and effectiveness suffer from the risk of being considerably resized. In particular, the interface with the EU IPRs enforcement regime deserves more attention. On point, this paper illustrated that the ambiguities left by the text of many portability-related provisions concerning such interface favour the under-implementation of portability, also due to the trend of increasing the liability threshold for content providers under Article 17 CDSMD. In this sense, more coordination would be welcome and may be useful to prevent the practical effect of portability rules being substantially frustrated.

Funding

This article received no funding

The cost of editing selected articles published in the Yearbook of Antitrust and Regulatory Studies in the 2022–2024 is covered by funding under the program "Development of scientific journals" of the Ministry of Education and Science under agreement No. RCN/SN/0324/2021/1. Task title: "Verification and correction of scientific articles and their abstracts". Funding value: 36 298,00 PLN; The task consists of professional editing of articles published in English.

Declaration of Conflict of interests

The author declared no potential conflicts of interest with respect to the research, authorship, and publication of this article.

Declaration about the scope of AI utilisation

The author did not use AI tools in the preparation of this article.

Literature

Akman P, 'Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act', European Law Review (2022), 47, 85, available at SSRN: <https://ssrn.com/abstract=3978625>.

Bakhoum M, Conde Gallego B, Mackenrodt MO, Surblytė-Namavičienė G (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. MPI Studies on Intellectual Property and Competition Law, (2018) vol 28. Springer, Berlin, Heidelberg.

Baschenhof P, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?' U Ill JL Tech & Pol'y (2022) 1.

Bongartz P, Langenstein S, Podszun R, 'The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers', Journal of European Consumer and Market Law, (2021), Vol 10, Iss 2, 60–67.

Borghi M, 'Data Portability and Regulation of Digital Markets', CIPPM / Jean Monnet Working Papers, (September 2019), Bournemouth University, available at SSRN: <https://ssrn.com/abstract=3617792>.

Cennamo C, Kretschmer T, Constantinides P, Alaimo C, Santaló J, 'Digital Platforms Regulation: An Innovation-Centric View of the EU's Digital Markets Act', Journal of European Competition Law & Practice, January 2023, Vol 14, Iss 1, 44–51.

De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Sanchez I, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services', Computer Law & Security Review, (2018), 193–203, Available at SSRN: <https://ssrn.com/abstract=3447060>.

De Streel A, Alexiadis P, 'The EU's digital markets act opportunities and challenges ahead', Business Law International, (2022), Vol 23, No. 2, 163–201.

Drexl J, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC' (2018) BEUC, 110.

Drexl J et al., 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public Consultation on Building the European Data Economy' (2017) *Max Planck Institute for Innovation & Competition* Research Paper No. 17-08, available at SSRN: <https:// ssrn.com/ abstract=2959924>, para 25.

Elfering S, 'Unlocking the Right to Data Portability. An Analysis of the Interface with the *Sui Generis* Database Right', (2022) in *MIPLC Studies*, No. 38, Max Planck Institute for Innovation and Competition, 11.

Engels S, Nordemann JB, 'The Portability Regulation (Regulation (EU) 2017/1128): A Commentary on the Scope and Application' JIPITEC (2018), 9, 179 para 1.

Etteldorf C, 'DMA – Digital Markets Act or Data Markets Act?' Eur Data Prot L Rev (2022), 8, 255.

Ferretti F, 'A Single European Data Space and Data Act for the Digital Single Market: on Datafication and the Viability of a PSD2-like Access Regime for the Platform Economy' Eur J Legal Stud, (2022), 14, 173.

Frosio G, 'Reforming the C-DSM Reform: A User-Based Copyright Theory for Commonplace Creativity', IIC (2020), 51, 709.

Frosio G, 'It's All Linked: How Communication to the Public Affects Internet Architecture' Computer Law & Security Review, (12 March 2022), 37.

Frosio G, 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe', Oxford Journal of Intellectual Property and Practice, (2017), 12, 565–575.

Frosio G, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy', Northwestern University Law Review, (2017), 112, 19.

Hondagneu-Messner S, 'Data Portability: A Guide and a Roadmap', Rutgers Computer & Tech LJ (2021), 47, 240.

Geiger C, Jütte BJ, 'Platform liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match', Gewerblicher Rechtsschutz und Urheberrecht International (2021), 70, 517.

Geiger C, Jütte BJ, 'Towards a Virtuous Legal Framework for Content Moderation by Digital Platforms in the EU? The Commission's Guidance on Article 17 CDSM Directive in the light of the *YouTube/Cyando* judgement and the AG's Opinion in C-401/19', EIPR (2021), 43:10, 625–635.

Geiregat S, 'Copyright Meets Consumer Data Portability Rights: Inevitable Friction between IP and the Remedies in the Digital Content Directive', GRUR International, (June 2022), Vol 71, Iss 6, 495–515.

Geradin D, Bania K, Karanikioti T, 'The Interplay between the Digital Markets Act and the General Data Protection Regulation' (29 August 2022), <https://papers.ssrn.com/ abstract=4203907>.

Gill D, Metzger J, 'Data Access through Data Portability: Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars' Eur Data Prot L Rev (2022), 8, 221.

Graef I, 'Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union', Telecommunications Policy, Vol 39, Issue 6, 502–514.

Graef I, 'The opportunities and limits of data portability for stimulating competition and innovation', Competition Policy International – Antitrust Chronicle, (2020) 2(2), 1–8.

Graef I, Tombal T, de Streel A, 'Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer', TILEC Discussion Paper, (November 27, 2019), No. DP 2019-024, Available at SSRN: <https://ssrn.com/abstract=3494212>.

Graef I, Husovec M and Purtova N, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', Tilburg Law School Legal Studies Research Paper Series, no. 22/2017, 6–7.

Graef I, Verschakelen J, Valcke P, 'Putting the right to data portability into a competition law perspective', (2023), The Journal of the Higher School of Economics, Annual Review, 53–63.

Husovec M, Quintais JP, 'How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive', Gewerblicher Rechtsschutz und Urheberrecht International, (2021), 70, 325–348.

Janal R, 'Data Portability – A Tale of Two Concepts', JIPITEC (2017), 8, 59 para 1.

Janal R, 'Data portability under the GDPR: A blueprint for access rights?', in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare*, (2021), Nomos, 319–342.

Jeon DS, Menicucci D, 'Data portability and competition: Can data portability increase both consumer surplus and profits?' Eur J Law Econ, (2024), 57, 145–162.

Krämer J, 'Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations', Journal of Competition Law & Economics, (2021) Vol 17, Iss 2, 263–308.

Kerber W, 'Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law', The Antitrust Bulletin, (2022), Vol. 67(2) 280–301.

Kerber W, 'Digital markets, data, and privacy: competition law, consumer law and data protection', Journal of Intellectual Property Law & Practice, (November 2016), Vol 11, Iss 11, 856–866.

Kuczerawy A, 'From 'Notice and Takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression', in G Frosio (ed), *The Oxford Handbook of Online Intermediary Liability*, (2020), Oxford University Press, 525-543.

Kuebler-Wachendorf S, Luzsa R, Kranz J, Mager S, Syrmoudis E, Mayr S, Grossklags J, The Right to Data Portability: conception, status quo, and future directions, Informatik Spektrum (2021) 44, 264–272.

Lazarotto B, 'The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act', EJLT, (2024), Vol 15, n 1, 1–15.

Lienemann G, 'Global Perspectives on the Right to Personal Data Portability: Surveying Legislative Progress and Propositions for User-Led Data Transfers', (April 21, 2023), available at SSRN: <https://ssrn.com/abstract=4427736>.

Lindroos KW, NHB Hang, 'The Portability Regulation', in I Stamatoudi, P Torremans, (eds), *EU Copyright Law*, 2nd ed, 575–609.

Lynskey O, Aligning data protection rights with competition law remedies? The GDPR right to data portability, European Law Review, (2017), 42 (6). 793–814.

Martinelli S, 'Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"', in L Reins (ed), *Regulating New Technologies in*

Uncertain Times. Information Technology and Law Series, vol 32. T.M.C Asser Press, The Hague.

Mazziotti G, 'Allowing online content to cross borders: is Europe really paving the way to a Digital Single Market?', in Pihlajarinne, T, Vesala J, Honkkila, O (eds), *Online Distribution of Content in the EU*, (2019) Edward Elgar Publishing, 188–203.

Metzger A et al., 'Data-Related Aspects of the Digital Content Directive', JIPITEC, (2018), 90, paras. 46–49.

Metzger A, Senftleben M, 'Understanding Article 17 of the EU Directive on Copyright in the Digital Single Market – Central Features of the New Regulatory Approach to Online Content-Sharing Platforms', Journal of the Copyright Society of the U.S.A. 67 (2020), 279 (284–308).

Moreno Belloso N, Petit N, 'The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove' European Law Review (2023), 48, 391, available at SSRN: <https://ssrn.com/abstract=4411743>.

Nicholas G, 'Taking It With You: Platform Barriers to Entry and the Limits of Data Portability', Mich Tech Rev. (2021), 27, 263, 272.

Nixdorf W, 'Planting in a Walled Garden: Data Portability Policies To Inform Consumers How Much (if any) of the Harvest is Their Share', Transnational Law & Contemporary Problems, (2020), Vol 29:135, 136–165.

Oprysk L, 'Digital Consumer Contract Law without Prejudice to Copyright: EU Digital Content Directive, Reasonable Consumer Expectations and Competition', GRUR International, October 2021, Vol 70, Iss 10, 943–956.

Picht PG, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, Further EU Digital Regulation Acts, and Competition Law', Journal of European Competition Law & Practice, March 2023, Vol 14, Issue 2, 67–82.

Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, *IPR and the use of open data and data sharing initiatives by public and private actors*, PE 732.266, May 2022, Study Requested by the JURI Committee for the European Parliament.

Purtova N, 'The law of everything. Broad concept of personal data and future of EU data protection law', Law, Innovation and Technology, (2018), 10:1, 40-81.

Quintais JP, Frosio G, et al., 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics', JIPITEC (2020), 10, 277–282.

Reda J, Selinger J, Servatius M, *Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment* (Study for Gesellschaft für Freiheitsrechte), (December 2020). Full text available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3732223>.

Riordan J, 'A Theoretical Taxonomy of Intermediary Liability', in G Frosio (ed), *The Oxford Handbook of Online Intermediary Liability*, (2020), Oxford University Press, 78.

Rubinfeld D, Gal M, 'Access Barriers to Big Data', Ariz L Rev, (2017), 59, 339, 364.+

Rubinfeld D, 'Data portability and interoperability: An E.U.-U.S. comparison', Eur J Law Econ (2024), 57, 163–179.

Schwemer SF, 'Article 17 at the Intersection of EU Copyright Law and Platform Regulation', Nordic Intellectual Property Law Review (2020), 400–435.

Scudiero L, 'Bringing Your Data Everywhere: A Legal Reading of the Right to Portability ', Eur Data Prot L Rev, (2017), 3, 119.

Senftleben M, 'Institutionalized Algorithmic Enforcement – The Pros and Cons of the EU Approach to Online Platform Liability', Florida International University Law Review (2020), 14, 299–328.

Senftleben M, 'Bermuda Triangle: Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market', EIPR, 2019, 41, 480.

Senftleben M, Angelopoulos C, et al., 'The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform', EIPR, (2018), 40, 149.

Synodinou TE, 'The Portability of Copyright-Protected Works in the EU', in TE Synodinou, P Jougleux, C Markou, T Prastitou, (eds) *EU Internet Law*, (2017), Springer, 217–266.

Swire P, Lagos Y, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' Md L Rev, (2013), 72, 335.

Syrmoudis E, Mager S, Kuebler Wachendorff S, Pizzinini P, Grossklags J, Kranz J, 'Data Portability between Online Services: An Empirical Analysis on the Effectiveness of Article 20 GDPR', Proceedings on Privacy Enhancing Technologies, 2021 (3), 351–372.

Tombal T, 'Imposing Data Sharing Among Private Actors. A Tale of Evolving Balances' (University of Namur 2021) para 154.

Urquhart L, Sailaja N, McAuley D, 'Realising the Right to Data Portability for the Domestic Internet of Things' [2017] <https://ssrn.com/ abstract=2933448> accessed 28 March 2018, 3.

Ursic H, 'Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control' SCRIPTed (2018) 15, 42.

Vereecken J, Werbrouck J, 'Goods with Embedded Software: Consumer Protection 2.0 in Times of Digital Content?' in D Wei, JP Nehf, CL Marques (eds), *Innovation and the Transformation of Consumer Law* (Springer 2020) 94.

Vezzoso S, 'Competition Policy in Transition: Exploring Data Portability's Roles', Journal of European Competition Law & Practice, May 2021, Vol 12, Iss 5, 357–369.

Voigt P, von dem Bussche A, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 383, 10.

Wong J, Henderson T, 'The right to data portability in practice: exploring the implications of the technologically neutral GDPR', International Data Privacy Law, (2019), Vol 9, Iss 3, 173–191.

Zanfir G, 'The right to data portability in the context of the EU data protection reform', International Data Privacy Law, (2012), Vol 2, Iss 3, 149–162.

Zhang J, 'The Paradox of Data Portability and Lock-In Effects', Harvard Journal of Law & Technology, Vol 36, No 2, 2023, available at SSRN: <https://ssrn.com/ abstract=4728972>.

Zufall F, Zingg R, 'Data Portability in a Data-Driven World', in S Peng S, CF Lin, T Streinz (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, Cambridge University Press; (2021), 215–234.