Data protection beyond data protection regulation

*Johanna Chamberlain and Andreas Kotsios**

1. Introduction

In recent years, data protection has become synonymous with the EU general data protection regulation[1] (GDPR), in force since 2018. However, data protection rules coexist with a number of other regulations that may enhance and complement but also, perhaps, cause confusion. In fact, personal data or sensitive information is – directly or indirectly – protected in many older and newer regulations that do not specifically belong to the area of data protection.

In this chapter we examine data protection from the individual's perspective, considering him or her as more than just – or at least not only as – a data subject. Our objective is to evaluate not just the GDPR but also the broader legal frameworks which may offer individuals alternative, and sometimes more suitable, protection against a party who processes his or her personal data in a way they find unacceptable. More specifically we will examine which data protection mechanisms can be identified in the areas of tort law and consumer law. We will also examine how the upcoming AI Act and some other related proposals from the Digital Decade Strategy may add to the protection of personal data and the interpretation of the GDPR.[2, 3] In this contribution we will thus

* Both authors are postdoctoral researchers at the Commercial Law Sector, Department of Business Studies, Uppsala University. The authors would like to thank WASP-HS for funding their research within the project "AI and the Financial Markets: Accountability and Risk Management with Legal Tools".

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L 119/1.

[2] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts, COM/2021/206 final (AI Act Proposal).

[3] Two other, more technically focused works on the relationship between data protection and AI are Kingston, 'Using artificial intelligence to support compliance with the general data protection regulation', 2017, 25 Artificial intelligence and law 4, pp. 429–443, and Andraško,

discuss how the chosen legal areas relate to rules on data protection,[4] when they overlap and if protection in certain situations is missing despite (or due to) the multitude of possible legal alternatives.

2. Data protection and consumer law

2.1 Introduction

We can probably all agree that for anyone working with data protection there is one piece of law that directly comes to mind, the GDPR. However, it has widely been argued that personal data as such are "the currency of today's digital market"[5], the raw material for added value services,[6] the "blood in the veins of the digital economy"[7] and the likes. If we are willing to accept that personal data are of importance for the economy or, even more so, that they directly have an economic value, it means that such economic value can change hands – as any other

---

Mesarčík & Hamuľák, 'The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework', 2021, 36 AI & society, 2021 2, pp. 623–636. See also Kuner, Cate, Lynskey, Millard, Ni Loideain & Svantesson, 'Expanding the artificial intelligence-data protection debate', 2018, 8 International data privacy law 4, pp. 289–292.

[4] For a general survey of the relationship between the GDPR and AI, see European Parliament study 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), June 2020. Our focus in this contribution can be described as the opposite of the EU study – namely, the impact of AI rules on data protection. However, see for instance p. 31 of the study, where it is stated that "AI may both promote and demote different fundamental rights and social values included in the EU Charter and in national constitutions", with the rights to privacy and data protection (Articles 7 and 8 of the Charter) at the "forefront". Further, on p. 32 the relationship between AI and existing legal areas is discussed: "Given the huge breadth of its impacts on citizens' individual and social lives, AI falls under the scope of different sectorial legal regimes. These regimes include especially, though not exclusively, data protection law, consumer protection law, and competition law. As has been observed by the European Data Protection Supervisor (EDPS) in Opinion 8/18 on the legislative package 'A New Deal for Consumers,' there is synergy between the three regimes." On the same page, "civil liability law relative to harm caused by AI driven systems and machines" is also mentioned as a connecting legal area.

[5] Reding, 'President of the European Commission, EU Justice Commissioner – The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation' (European Commission, 22 January 2012, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26).

[6] Lieshout, 'The Value of Personal Data' in Camenisch, Fischer-Hübner & Hansen (eds), *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, Vol. 457 (Springer International Publishing 2015), http://link.springer.com/10.1007/978-3-319-18621-4_3.

[7] Lohsse, Schulze & Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy* III, 1 st edition (Nomos, 2017), p. 15; Recital 13 of the Proposal for a Directive of The European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content COM(2015) 634 Final.

economic value – in exchange for other valuable things, like digital products and digital services.[8] In that case the economic interests of consumers, namely whether, what and under what conditions to make purchases, are directly related to the processing of consumers' personal data and consequently, consumer law becomes applicable in order to protect these interests.

The reason why personal data are seen as so valuable is because processing these personal data enables traders to understand the behaviour of consumers, and therefore either provide products and services that are closer to the wishes of consumers or directly or indirectly affect these wishes. In that sense, the processing of personal data is related to the decisions that are taken by consumers with regard to products and services, and therefore consumer law again becomes important for the protection of such choices as well as regarding the consequences of such choices.

For these reasons, at least some questions related to the processing of personal data have for the past 10 years also been regarded as matters of consumer law.[9] By examining the literature as well as the decisions by consumer authorities and national courts in the EU,[10] we will illustrate how consumer law has been used as a complement to data protection legislation in order to tackle issues that are related to the broader data protection problems. In some cases, we may detect some overlap but there are also cases where we find that consumer law has an added value as an instrument that broadens the scope of data protection either because it directly addresses a problem that the GDPR does not, or because it can be used as an interpretative tool for the GDPR.

In order to achieve this objective, we will focus on obligations related to the conditions for the processing of personal data posed on traders. We divide these obligations into those related to provision of information, obligations on refraining from specific actions and lastly obligations on acting in a specific manner.

[8] For a critique of this approach to personal data see EDPS Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016, p. 8, where the European Data Protection Supervisor (EDPS) compared the market for personal data with a market for human organs. For a general critical approach on the relationship between consumer and data protection law see Kotsios, *Paying with Data: A Study on EU Consumer Law and the Protection of Personal Data* (Department of Law 2022).

[9] Kotsios, *Paying with Data: A Study on EU Consumer Law and the Protection of Personal Data* (Department of Law 2022), pp. 34–35.

[10] The alignment of the data protection and consumer protection policy agendas is being increasingly discussed in academic literature, policy making and enforcement circles; see Clifford, 'Data Protection and Consumer Protection: The Empowerment of the Citizen Consumer' in González-Fuster, Van Brakel & De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing 2022).

2.2 Obligations to provide information related to the processing of personal data

EU consumer law has in general used information as its main tool for protecting consumers through enabling them to take free, well-informed decisions.[11] After all, a main narrative in this area of law has been that the information costs for consumers are higher than for traders and therefore law should address this imbalance.[12] The three main EU directives in consumer law – that are not sector-specific – defining the information obligations of traders have been the Consumer Rights Directive (CRD)[13], the Unfair Commercial Practices Directive (UCPD)[14] and the Unfair Contract Terms Directive (UTD)[15].

These directives pose obligations on traders to provide specific information to consumers. Even though there is no explicit mention of information related to the processing of personal data we can nevertheless detect some provisions of relevance. Firstly, according to the CRD traders must provide information related to the functionality of a digital product or service; and secondly, according to the UCPD traders must also provide any information that may enable consumers to take a well-informed transactional decision, namely "any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting"[16]. Here we may also add that the UTD also demands that traders provide *transparent* infor-

[11] We may point out here that it has even been claimed that information has been the "singularly important element in the regulatory toolbox", see Helberger, 'Diversity Label: Exploring the Potential and Limits of a Transparency Approach to Media Diversity', 2011, 1 Journal of Information Policy 337, p. 337.

[12] See here indicatively Seizov and others, 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU', 2019, 42 Journal of Consumer Policy 149, p. 152 and references. The CJEU has also expressed this idea (see Joined Cases C-54/17 and C-55/17, *Wind Tre*) where it referred to the fact that 'the consumer is in a weaker position, particularly with regard to the level of information' (para. 54).

[13] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L 304/64.

[14] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L 149/22.

[15] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.

[16] Article 2(k) of the UCPD.

mation in the sense that consumers, through information, should be enabled to understand the terms of a contract and its consequences.[17]

Starting with the CRD, it is important to note that it was one of the first pieces of EU law which, even though not being focused on the protection of personal data, recognised – indirectly in the beginning – this rather new phenomenon where consumers may "purchase" products without the provision of money but instead in exchange for their data. This at least was the case for purchases of digital content, since the CRD did not relate such "purchases" to sales or services contracts, which can only be concluded with a payment.[18] This means that the information obligations provided under the CRD are posed on traders even if the consumer has not paid any price in money, as long as the trader supplies digital content; and after the Modernisation Directive,[19] which amended the CRD, even when providing digital services.[20] The latter directive also explicitly states that the CRD is to apply directly as soon as consumers provide their personal data for reasons that are not exclusively related to the supply of the digital content or service.[21] The processing of personal data then when this is done in order to monetise the data, triggers the application of the CRD in general and traders must provide all relevant information to consumers.

From this information, one provision that is of importance and could potentially be used in order to protect consumers not only with regard to their purchase but also with regard to the processing of their data, can be found in Article 6(1)(r) of the CRD. This provision obliges traders to provide information about the functionality of a product. The Com-

[17] See for example Case C-186/16 *Ruxandra Paula Andriciuc and Others v Banca Românească SA* [2017], EU:C:2017:703, para. 48.

[18] This was implied in the Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, which referred to the "value" and "price" of the goods, and Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts referring to payments. In this context, claiming that the provision of personal data is a payment becomes a rather controversial statement. The recitals of the Modernisation Directive indicate that there is a clear distinction between payments, which ask for the provision of money, and the provision of personal data, Recital 31 of the Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

[19] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7.

[20] After the Modernisation Directive there is a new article in the CRD, Article 3(1a), which leaves no doubt that it also contains such transactions.

[21] Article 3(b) of the CRD.

mission declared in its guidance document that functionality is related to tracking and personalisation.[22] What that means in practice and how much information should be provided is not exactly clear, but Article 2(11) of the Digital Content Directive (DCD) provides some clarification by stating that functionality calls attention to "the ways in which digital content or a digital service can be used"[23]. In that sense the main question here is if a digital product can fulfill its purpose or not. Even though the example given under the DCD is about Digital Rights Management mechanisms (DRMs) it would make sense to extend this reasoning also to products that, for example, are created exactly to protect consumers' personal data such as VPN services that are by definition created in order to encrypt communication. If such services do not provide an adequate level of encryption they cannot be used as expected – or at least they are used under a misconception. Similarly, any personalisation that is directly related to how a product or service is to function should be provided by the trader.

The depth of this information, meaning how much detailed information has to be provided, would now probably be related to what is needed by the consumer in relation to this functionality. In most cases a mere reference to the fact that a service is personalised, based on for example the previous interaction of a consumer with an app, would probably suffice from a consumer law point of view, since this information would enable the average consumer to take a decision related to the personalised product or service.[24] In most cases then the information that has to be provided according to the CRD will probably be less comprehensive than the information found under the GDPR. Nevertheless, the obligation to provide information related to the processing of personal data as part of the functionality of a digital product or a service under the CRD should be considered as an extra safeguard for the protection of personal data. This goes especially for the case of information related to what security measures are embedded in a product, e.g. what kind of encryption is used in VPN services, information that is not

[22] Commission, 'Guidance Document Concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, Amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council' (June 2014).

[23] Article 2(11)of the DCD in connection to Recital 43.

[24] Of course, arguments can be made here that consumers would probably want some more information on how personalisation works but we have to keep in mind that in consumer law the question is rather what information is *needed* by the average consumer and not merely *wanted*. However, this is a subject for another paper. See further Kotsios, *Paying with Data: A Study on EU Consumer Law and the Protection of Personal Data* (Department of Law 2022) p. 211.

required to be provided to data subjects under the GDPR – even though a data controller has to implement security measures.

Except for the CRD and the information that is related to the functionality of a product, in EU consumer law we find also the UCPD that asks for the provision of *any* information that is *needed* by consumers in order to make well-informed transactional decisions. As has rightly been claimed, the UCPD provides for a general duty of information across EU consumer law.[25] Except for the above information that is related to the functionality of a product, it has been argued that the UCPD could also be used to provide for some added information obligations with regard to the processing of personal data. This would be the case since the UCPD does not define in detail what information has to be provided to consumers, but instead states that all information necessary for an average consumer to make an informed transactional decision should be provided. A number of scholars and consumer authorities have claimed that the UCPD is a good complement to the protection of personal data and based this argument on two main premises: That consumers need to know a) whether their data have been used as a payment and b) how their data have been used in case of personalised advertising and pricing.[26]

With regard to the former, the main argument for its application has been based upon clause No 20 of Annex I of the UCPD which states that a product should not be described as "gratis", "free", "without charge" or similar "if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item". Therefore, as this argument goes, traders claiming that consumers do not provide anything in exchange for a service, act against this provision of the UCPD considering that they mon-

[25] Durovic, *European Law on Unfair Commercial Practices and Contract Law* (Hart Publishing 2016) p. 110.

[26] Indicatively, see Rhoen, 'Beyond Consent: Improving Data Protection through Consumer Protection Law', 2016, 5 Internet Policy Review (https://policyreview.info/node/404) accessed 16 March 2021; van Eijk, Jay Hoofnagle & Kannekens, 'Unfair Commercial Practices', 2017, 3 European Data Protection Law Review 325; Helberger, Zuiderveen Borgesius and Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law', 2017, 54 Common Market Law Review 1427; Helberger and others, 'Surveillance, Consent and the Vulnerable Consumer. Regaining Citizen Agency in the Information Economy', EU Consumer Protection 2.0 – Structural Asymmetries in Digital Consumer Markets (BEUC 2021); Koops, 'The Trouble with European Data Protection Law', 2014, 4 International Data Privacy Law 250; AGCM, PS10601 – WhatsApp – Trasferimento Dati a Facebook [2017] Provvedimento n. 26597; AGCM, PS11112 – Facebook-Condivisione Dati con Terzi [2018] Provvedimento n. 27432; Hungarian Competition Authority, 'Competition Proceeding against Google Is Closed with Commitment Decision' (GVH, 31 August 2018, gvh.hu/en/press_room/press_releases/press_releases_2018/competition_proceeding_against_google_is_closed); Competition and Markets Authority, 'Online Dating Services' (GOV.UK, 13 June 2018).

etise the data of consumers. Likewise, it has been argued that failing to state that personal data are used for commercial purposes can also be considered as a "by definition" unfair practice described in clause No 22 of the Annex I of the UCPD, which bans practices where traders give the false impression that they do not act for purposes that are related to their trade or profession, namely when they hide their commercial intention.

More specifically, this line of argumentation has been used by some national consumer authorities when deciding whether traders that process personal data for commercial purposes have been acting against the provisions of the UCPD. One of the most active authorities when it comes to applying consumer law for data protection has been the national consumer authority in Italy, the Italian Competition Authority (AGCM). Already in 2000, the AGCM found that an advertisement regarding a free subscription to online services was misleading because consumers accepted a "passive" obligation to "provide personal data in exchange for a service"[27] and in that sense the trader did not provide information about the price and generally the conditions under which the service was supplied. The AGCM in this way recognised the economic value of personal data and the need to protect consumers with regard to this value. 17 years later, in 2017, the AGCM fined WhatsApp using the provisions of Italian law corresponding to Articles 5, 8 and 9 of the UCPD because the trader "implemented [unfair practices] through a) an emphasis on the need to subscribe to the new conditions within the following 30 days, failing which they would have lost the opportunity to use the service; b) inadequate information on the option of denying consent to share personal data with Facebook; c) the preselection of the option to share the data (users should deselect the box to opt-out)". Here, the main idea was again that personal data have an economic value and therefore the UCPD may apply and more specifically that "the data of WhatsApp users, utilised for the profiling of the users for commercial and marketing purposes acquire an economic value suitable to qualify the behaviour as a commercial practice"[28].

[27] AGCM, PI2686 – Libero Infostrada [2000] Provvedimento n. 8051. Directorate for Financial and Enterprise Affairs and Competition Committee (n. 772) 3–4 referring to Libero Infostrada. The case was before the adoption of the UCPD but was based on the national implementation of the Directive 84/450/EEC on misleading advertising and its Article 3(b) on the obligation to provide information about the price and how this price is calculated. As we claimed in the beginning of this chapter, the discussion on the use of consumer law for issues related to data protection has only been ongoing for the past 10 years approximately.

[28] Directorate for Financial and Enterprise Affairs and Competition Committee, 'Quality Considerations in the Zero-Price Economy – Note by Italy', 2018 (https://one.oecd.org/document/DAF/COMP/WD(2018)148/en/pdf), p. 5. See also BEUC, 'What's up with WhatsApp? An Assessment of WhatsApp's Practices in the Light of EU Consumer Protection Rules' (2021)

Similarly, in 2018 the AGCM fined Facebook for a number of violations of the Italian law implementing the UCPD. According to the AGCM, Facebook should not claim that it is "free and will always remain free" since this claim is misleading and makes consumers take a transactional decision which they may otherwise not have taken. The interesting point here is that Facebook took the case to the court but both the first and second instance courts reasoned similarly to the Italian consumer authority, recognising again the economic value and commercial significance of personal data.[29] Similar to the above interpretations of the UCPD, the JURI Committee in its study on the UTD and digital markets found that terms "creating the impression that digital services are provided for free, where consumers are paying for the service with their personal data, time or attention", should be deemed unfair.[30]

BEUC, which is an umbrella group for consumer organisations in Europe, has also pointed out the possibility to apply the UCPD and the UTD on the grounds that traders many times do not provide the information that consumers need or they mislead consumers with the information they provide. In 2021 it submitted an external alert to the European Commission arguing that WhatsApp does not explain in *plain and intelligible language* the nature of the changes in its privacy policy and their consequences for users with regard to how their personal data are shared with Facebook and third parties.[31] The importance of transparency requirements of the UTD, namely the obligation to provide information in a plain and intelligible language, as a tool for the interpretation of the transparency requirement in the GDPR has even been embedded in the recitals of the GDPR. In Recital 42 we find that "declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms". Now this recital has triggered some academic debate on its meaning and how it should be

---

pp. 12–16 (https://www.beuc.eu/publications/beuc-x-2021-063_report-whats_up_with_whatsapp.pdf), that also investigated the same matter.

[29] As has already been said this approach is not undeniable and it is rather characteristic that in Germany a court made apparent that claiming that Facebook is and will remain free does not constitute a misleading practice, since the question of what is free or not means whether a cost is imposed on one of the parties or not and costs are to be understood as pecuniary charges. Any "purely immaterial interests" such as the right to information self-determination cannot be understood as such costs. LG Berlin, Urteil vom 16.01.1018 – 16 O 341/15 (n. 134).

[30] Loos & Luzak, 'Update the Unfair Contract Terms Directive for Digital Services' (Parliament's Committee on Legal Affairs (JURI) 2021), p. 7.

[31] BEUC, 'What's up with WhatsApp? An Assessment of WhatsApp's Practices in the Light of EU Consumer Protection Rules' (2021) pp. 12–16 (https://www.beuc.eu/publications/beuc-x-2021-063_report_- _whats_up_with_whatsapp.pdf).

interpreted,[32] but for the purposes of this paper it suffices to conclude that the EU legislator has found the existing interpretation of the transparency requirement under the UTD to be useful as a tool for the interpretation of the GDPR.

To summarise, there are several arguments for the implementation of consumer law and especially the UCPD with regard to information that must be provided by traders related to the not-so-free nature of purchases done with the "provision" of personal data. These arguments include first that consumers become more aware of the importance of their data in general. Drawing the attention directly to this commercialisation is not the task of the GDPR and consumer law adds an important nuance that is missing in data protection legislation. Second, when it comes to information that has to be provided as part of the transparency principle in EU consumer law, the UCPD and the UTD – together with the CRD – can be understood as demanding the provision of information related to the security measures that traders implement for the protection of personal data. As stated above, the CRD may pose such an information obligation if security is part of the functionality of the product. However, even if it is not, information about such measures may nevertheless be information *needed* by consumers since, under the UCPD, it enables consumers to take a transactional decision or, under the UTD, to understand the consequences of the terms of a contract.[33] Such information is not required to be provided under the GDPR, and therefore the consumer law acquis can in this case be of great help for the promotion of more secure digital products that process personal data. This is the case because traders, by being transparent on what security measures they deploy, enable consumers to take well-informed decisions which even though they are related to their economic interests, namely what products to purchase and use, nevertheless affect the protection of their fundamental rights.

[32] Bygrave, 'Article 4(11) Consent' in Kuner and others (eds), *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles* (2021), p. 47; Clifford, Graef & Valcke, 'Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections', 2019, 20 German Law Journal 679, p. 687; Svantesson, 'Enter the Quagmire – the Complicated Relationship between Data Protection Law and Consumer Protection Law', 2018, 34 Computer Law & Security Review 25, p. 7.

[33] Kotsios, *Paying with Data: A Study on EU Consumer Law and the Protection of Personal Data* (Department of Law 2022), p. 233.

2.3 Obligation to refrain from certain actions

Except for information obligations, EU consumer law also imposes an obligation on traders to refrain from certain actions. The actions that traders have to refrain from are commercial practices that may affect consumers' ability to take transactional decisions. Such practices are either misleading ones, that are more related to what information is provided and how – something that we talked about above – or aggressive practices, namely practices that entail some kind of harassment, coercion or undue influence.[34]

Most arguments related to the application of consumer law for the protection of consumers' personal data in this case are based on Article 2(j) of the UCPD and more specifically on the prohibition to unduly influence consumers. According to this provision, aggressive commercial practices are the ones that "exploit[ ] a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision". Now even though the CJEU has not interpreted this provision except for very few cases – which in the end were more about the information that was provided to consumers –[35] some scholars and consumer authorities have nevertheless claimed that this provision should apply also in cases where consumers are influenced into accepting terms related to the processing of their personal data.

Mulders and Goanta claim, for example, that especially in the context of social media, consumers cannot be considered to make a free choice to use or not to use such social media since the truth is that "we need them in order to be in contact with friends, co-workers, family and so on". Therefore, when it comes to accepting the terms and conditions of such traders, according to them, this choice is made under pressure. They thus find that this *structural* power imbalance[36] between consum-

[34] Article 8 of the UCPD.

[35] There are three cases on the matter: Joined Cases C-54/17 and C-55/17 *Autorità Garante della Concorrenza e del Mercato v Wind Tre SpA*, *Vodafone Italia SpA* [2018], EU:C:2018:710, Case C-428/11 *Purely Creative Ltd and Others v Office of Fair Trading* [2012], EU:C:2012:651; and Case C-628/17 *Prezes Urzędu Ochrony Konkurencji i Konsumentów v Orange Polska SA* [2019], EU:C:2019:480. For some critique on how aggressive practices have been interpreted by the Court and the focus on information see Helberger and others, 'Surveillance, Consent and the Vulnerable Consumer. Regaining Citizen Agency in the Information Economy', EU Consumer Protection 2.0 – Structural Asymmetries in Digital Consumer Markets (BEUC 2021), p. 67; Willett, 'Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive' (n. 690), p. 260.

[36] Important however to point out here is that the cases related to this provision in front of the CJEU have not taken into consideration the structural imbalance between a specific type of trader and consumers, but instead have focused on the relational imbalance that was created in a specific case.

ers and social media should be addressed through the application of the UCPD. These structural asymmetries, which are created by "the digitally mediated relationship, the choice architecture, the architectural infrastructure, and the knowledge structure" and the possibility to address them through the provisions of undue influence have also been pointed out by Helberger and others.[37]

This argument was also adopted by the BEUC in its above-mentioned alert to the Commission, claiming that WhatsApp in practice psychologically blackmailed consumers to accept the processing of their personal data, by sending recurrent notifications that consumers would not have access to the service and by not providing the possibility to opt-out from such notifications. Such practices were found by BEUC to be aggressive under the UCPD, since "[a]lthough, in theory, users could decide to turn to other messaging apps, quitting WhatsApp would be at the expense of losing most of their contacts. For many people, leaving WhatsApp is not an option because of the strong network effects and the lack of interoperability with other messaging services. For many, WhatsApp is the main channel for staying in touch with family and friends".[38]

Similarly, the AGCM when assessing the practices of WhatsApp after its acquisition by Facebook, found that WhatsApp "de facto *forced* the users of its service WhatsApp Messenger to accept in full the new Terms of Use, and specifically the provision to share their personal data with Facebook, by making them believe that without granting such consent they would not have been able to use the service anymore" [emphasis added][39]. In order to do that, according to the AGCM WhatsApp implemented the following four practices: a) an in-app procedure for obtaining the acceptance of the new Terms of Use characterised by an excessive emphasis placed on the need to subscribe to the new conditions within the following 30 days or otherwise lose the opportunity to use the service; b) provision of inadequate information on the possibility of denying consent to share the personal data on the WhatsApp account with Facebook; c) the pre-selection of the option to share the data; and finally d) a difficult process of effectively activating the opt-out option once the Terms of Use were accepted in full. Similarly, the same authority found in the Facebook case mentioned above that Facebook caused

[37] Helberger and others, 'Surveillance, Consent and the Vulnerable Consumer. Regaining Citizen Agency in the Information Economy', EU Consumer Protection 2.0 – Structural Asymmetries in Digital Consumer Markets (BEUC 2021), p. 70.
[38] BEUC, 'What's up with WhatsApp? An Assessment of WhatsApp's Practices in the Light of EU Consumer Protection Rules', 2021, 12–1, p. 9.
[39] Italian Competition Authority, 'WhatsApp Fined for 3 Million Euro for Having Forced Its Users to Share Their Personal Data with Facebook', 2017, Press Release (https://en.agcm.it/en/media/detail?id=a6c51399-33ee-45c2-9019-8f4a3ae09aa1).

undue influence to consumers by pre-selecting the broadest consent to data sharing, since when consumers opt-out of such sharing "they are faced with significant restrictions on the use of the social network and third-party websites/apps, which induce users to maintain the pre-selected choice".[40]

The above-mentioned practices have often been characterised as dark patterns that traders may deploy in order to affect consumers' choices.[41] What is important to point out here is that dark patterns refer not so much to the information that is provided by traders, but instead to the architecture and design elements that are used. As such they may affect consumers either by misleading them, for example by making certain decisions more prominent, or by aggressively imposing specific choices, such as by "shaming"[42] or "blinding"[43] consumers. More importantly, as the BEUC has pointed out, many companies design their choice architecture in a way that can create what is known as "click-fatigue", namely architectures where the decision to have a more privacy-friendly service requires many more steps than the less privacy-friendly ones – something that is often the case when it comes to cookie policies.[44]

The Digital Services Act (DSA)[45] now includes an operational definition in its recitals on what should be understood as dark patterns, which include the findings of the AGCM as well as the recommendations by the BEUC. More specifically it states that traders should be "prohibited from deceiving or nudging" by the use of "visual, auditory or other components" that lead consumers to make decisions that are not in their interest. Similarly, traders should be prohibited from repeatedly "requesting a recipient of the service to make a choice where such a choice has already been made, making the procedure of canceling a service significantly more cumbersome than signing up to it, or making certain choices more difficult or time-consuming than others, making it unreasonably difficult to discontinue purchases or to sign out from

[40] Italian Competition Authority, 'Facebook Fined 10 Million Euros by the ICA for Unfair Commercial Practices for Using Its Subscribers' Data for Commercial Purposes', 2018, Press Release. We may detect here that the AGCM does not adopt the same structural asymmetry argumentation, since the problem here according to the authority was that if traders did not employ the specific practices in the specific relationship, consumers would have been able to react even though the traders had market power.

[41] BEUC, '"Dark Patterns" and the Consumer Law Acquis – Recommendations for Better Enforcement and Reform', BEUC-X-2022-013 – 07/02/2022.

[42] By creating guilt or peer pressure, see ibid. p 5.

[43] By pre-making choices for consumers in a rather sneaky way, see ibid.

[44] Ibid, pp. 7–8.

[45] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

a given online platform allowing consumers to conclude distance contracts with traders, and deceiving the recipients of the service by nudging them into decisions on transactions, or by default settings that are very difficult to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice."[46] What is important here is that the DSA effectively clarifies how the UCPD should understand such commercial practices.

If we combine the above with the not so new but nevertheless increasingly popular idea (especially in the case of consumer protection in digital environments) of interpreting the average consumer requirement of the UCPD – and the EU consumer law in general – through the lenses of digital vulnerability,[47] we may see that the UCPD could potentially cover a number of aggressive practices exactly because of the existing "digital asymmetry" between the parties. It is indicative of this asymmetry that a study by the Commission showed that 97% of EU traders deploy some kind of dark pattern, meaning some design element that is difficult to be understood and traced by consumers.[48]

Lastly, when it comes to actions related to the processing of personal data which traders should refrain from, it is worth mentioning the interpretation given to the UTD in some situations where the terms of a contract are related to the processing of personal data, since according to the UTD traders should not impose unfair terms to consumers. According to a study by the JURI Committee some terms that should be deemed unfair under the UTD include the ones "allowing DSPs to retain the collected personal data when consumers do not conclude a contract or the DSP terminates the contract or allowing DSPs to collect more personal data throughout the performance of the contract than what parties have originally agreed to, without the DSP notifying consumers about the change of the contract and giving them an option to terminate the contract" as well as the ones "limiting or excluding the access to digital services, if consumers do not give an explicit consent to the sharing of personal data in the scope exceeding what is needed for the provision of a digital service, including as a counter-performance for

[46] Recital 67 of the DSA.

[47] Galli, 2022, 'Digital Vulnerability'. In: *Algorithmic Marketing and EU Law on Unfair Commercial Practices. Law, Governance and Technology Series*, Vol 50. Springer, Cham. (https://doi.org/10.1007/978-3-031-13603-0_7); Helberger, Sax, Strycharz et al., 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability', 2022, Journal of Consumer Policy 45, 175–200 (https://doi.org/10.1007/s 10603-021-09500-5).

[48] European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, Boluda, Bogliacino et al., 'Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: Final report', Publications Office of the European Union, 2022 (https://data.europa.eu/doi/10.2838/859030).

the provision of digital services"[49]. The JURI Committee recommended that Article 1(l) of the Annex of the UTD should also include the cases where traders increase the amount of data acquired from consumers especially when these data come from third party sources. The JURI committee referred to the practice deployed by Facebook, which was examined by a German court under the competition law framework, where it gathered also off-Facebook user data. This change in "price", namely the processing of the additional data, should, according to the committee, be regarded as an unfair term and consumers should be given a clear option to terminate the contract.

It is important to note that the above interpretations have not been ascertained by the CJEU and there are a number of problems related to how broad these interpretations are in comparison to the existing ones made by the Court. Nevertheless, the above arguments show that especially in the case of dark patterns consumer law could have an added value.

2.4 Obligation to act in a specific manner

A third group of – positive – obligations posed by consumer protection legislation that is less discussed but nevertheless relevant for the protection of personal data through consumer law, is the provisions related mainly to the cybersecurity elements of consumer products and services. When it comes to the relationship between data protection and cybersecurity, even though data protection and data security are not the same thing there are undoubtedly a number of contact points.[50] Their common themes are expressed best in Article 5(1)(f) of the GDPR and the specification of this article in Articles 24, 25 and 32 with regard to the technical and organisational measures that data controllers must have in place when processing data.

Consumer law also contains a number of important provisions related to security which we here argue can add to the understanding of security as part of the personal data protection framework. Firstly, the Digital Content Directive (DCD) – and its twin directive on sale of goods (Consumer Sale of Goods Directive)[51] – explicitly asks for security in consumer products, while another important piece of consumer pro-

[49] Loos & Luzak, 'Update the Unfair Contract Terms Directive for Digital Services' (Parliament's Committee on Legal Affairs (JURI 2021), p. 7.
[50] Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context', 2022, 8 Oslo Law Review 126.
[51] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

tection legislation, the GPSD, defines what constitutes a safe product in the EU.

Starting with the DCD, it states in Article 8(1)(b) that digital content and services should be secure and this security should be one that is *normal* or one that consumers *reasonably expect* to be in place. In that sense security is not a mere secondary consideration but a main element of the performance features of a product or service, and consequently a matter of conformity of a product. As such, and considering that security and the protection of personal data go hand in hand when it comes to protecting such data from potential cyberattacks, consumer law could be used in order to define what kind of security should be deployed in order to protect such data.

There is of course an issue related to what is normal in a specific sector as well as to what consumers may expect for security. Of course, we all expect that products and services are safe and secure but the question is to what level, considering that in security there are tradeoffs which consumers normally cannot know. This question has not been answered by the CJEU but new legislative initiatives in the area of cybersecurity law, which we will discuss in the last part of this section, could be used in order to understand what consumers could reasonably expect for security in products and services: The security that is required by cybersecurity regulations.

The other main consumer law instrument that has been related to security is the GPSD, which for years has been the main tool for safe products in the EU. In general, safety in products has been understood as the prevention of physical harm. However, when it comes to other types of harm, as well as whether safety also includes security of products, the situation is rather blurry. This lack of clarity has been depicted in a report on how the GPSD has been implemented in the Member States. One of the questions was whether security issues related to modern products are covered under the directive. In some Member States it seems that such security risks are also included in the national laws implementing the directive while in others this is not the case; and in some third ones like in Germany, there seems to be great difficulty in saying whether the directive covers such risks and who the responsible authority is.[52]

However, the proposal on a new Product Safety Regulation has made clear that there is a will to also include security risks under the safety

[52] European Commission, 'Study for the preparation of an Implementation Report of the General Product Safety Directive – Final report' [2020]. Directorate General for Justice and Consumers.

umbrella.[53] This can also be found in an opinion of the "Sub-group on AI, connected products and other new challenges in product safety" in 2020, where we can read that even cases that are not directly related to physical harm and are actually about the security of a product could be covered by the GPSD. The example mentioned was a decision by the Icelandic authorities finding "that the product (a smartwatch) would not cause a direct harm to a child wearing it", meaning a physical harm, "but as the mobile application of the product lacked a minimum level of security, it could be easily used to have access to a child and potentially cause harm."[54] The main argument in this case was that a smartwatch is made exactly in order to "keep the child safe" and therefore lack of security and access to the data of the device by malevolent actors should not be allowed. If access to data through a product can lead to for example anxiety and depression, then this could also probably be understood as a safety matter. Therefore, products that need data to function should also provide for adequate security measures – otherwise, traders run the risk of putting products that are not safe on the market.

2.5 Summarising consumer law

The above discussion has shown that consumer law may be used to protect consumers' personal data directly or indirectly. While much of the protection that is provided overlaps the GDPR, it is relevant to highlight that some applications of consumer law may broaden the protection provided to individuals. Here, it is important to understand that even if some of the protection provided by the consumer law acquis can already be found under data protection legislation, such as in the cases of some misleading or aggressive practices that could actually be tackled also under the GDPR, consumer law adds an extra level of protection. This is mainly because consumer law makes it more difficult for traders to argue that under the GDPR they have a legitimate reason to deploy a commercial practice that is related to the processing of personal data for a purpose that is found to be unfair under consumer law.

[53] Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council COM/2021/346 final.
[54] European Commission, Opinion of the Sub-Group on Artificial Intelligence (AI), Connected Products and Other New Challenges in Product Safety to the Consumer Safety Network [2020].

3. Data protection and tort law

3.1 The Swedish Data Act

There has always been a close relationship between tort law and data protection, especially in Sweden. Already in the Swedish Data Act of 1973[55] – the first nationally applicable data protection law in the world – there was a clause on damages for wrongful treatment of personal data, § 23. The liability form was strict, and both pecuniary and non-pecuniary damages were compensable. This design is still reflected in the most up to date data protection regulation: The current GDPR and its Article 82 on damages, which means that the Swedish legislator was well ahead of the global development with the enactment of the 1973 Data Act.[56] Its generous model for damages resulting from data protection breaches is interesting in comparison to the general status of non-pecuniary damage in Swedish tort law, which was not as strong at the time – and the coverage of non-pecuniary damage was indeed debated in the preparatory works leading up to the Swedish Data Act.[57] The choice of strict liability was, in turn, motivated by the fact that automated data processing entailed large-scale spreading of (inaccurate) personal data and that mistakes regarding data treatment could happen without any possible identification of fault.[58] In sum, tort law's reparative function; to compensate victims of harm, appears to have been the main motivation for the chosen wording of § 23 of the Swedish Data Act.

According to the committee preparing the Swedish Data Act, compensation would primarily be needed when harm had been caused to an individual following registration without a permit, or through wrongful distribution of data.[59] The damages clause in the Swedish Data Act resulted in compensation of 500–5 000 SEK during the 25 years it was in force, with a few exceptions up to 10 000 SEK.[60] As will be discussed further below, the levels of compensation are not particularly high. Nevertheless, the tort law provision of the Swedish Data Act was an important part of the data protection regime from the start.

[55] Datalag (1973:289). For some background on the regulatory process and a description of the law's content, see Chamberlain, *Integritet och skadestånd* (Iustus 2020), pp. 104–107.
[56] For a comparative analysis of non-pecuniary harm and Article 82 GDPR, see Knetsch, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases', 2022, 13 Journal of European Tort Law 2, pp. 132–153.
[57] See preparatory work proposition 1973:33, pp. 146–147.
[58] Preparatory work proposition 1973:33, p. 148.
[59] Preparatory work SOU 1972:47, pp. 92–93.
[60] See Chamberlain, *Integritet och skadestånd* (Iustus 2020), p. 107.

3.2 The Damages Act

As mentioned above, the damages clause in the Swedish Data Act was progressive when it was enacted and especially so regarding the issue of non-pecuniary damage. A traditional principle of Swedish tort law is that non-pecuniary losses require specific legal bases in order to be compensable – thus differing from pecuniary harm, where there is no such condition.[61] Apart from clauses in specialised regulations, such as the tort law provision of the Swedish Data Act, the main legal base for non-pecuniary damage in the Swedish Damages Act[62] is Chapter 2, § 3. In essence, this provision regulates compensation for serious violations through crimes against certain protected interests: Persons, freedom, privacy and honour. It is notable that the violation must be "serious", as well as the result of a criminal action against at least one of the protected interests just mentioned. This means that tort law is completely dependent on criminal law when it comes to protecting, for example, invasions of privacy.

From a historically slow and almost reluctant development regarding the protection of privacy, during the latest decade the Swedish legislator has advanced a more active approach to data protection – partly as the result of judgments from the European Court of Human Rights.[63] Starting in 2013, several relevant clauses have now been enacted in Chapter 4 of the Swedish Criminal Code,[64] where crimes against privacy are regulated: ID theft (Chapter 4, § 6 b), secret filming and photographing in certain intimate environments (Chapter 4, § 6 a), spreading certain sensitive information (Chapter 4, § 6 c). Other clauses on for example molestation, threat and insult have been updated to better suit the digital age. Together, these amendments have filled most existing gaps in the criminal law protection of privacy and the new clauses are frequently used as legal base for damages claims regarding non-pecu-

[61] For an interesting discussion on tort law gaps in Member State legal orders, specifically regarding compensable non-pecuniary harms in relationship to AI risk regulation, see Li, 'Risk regulation and tort damage in the era of AI: Status quo and gaps' (https://blog.ai-laws.org/risk-regulation-and-tort-damage-in-the-era-of-ai-status-quo-and-gaps/), 29 January 2023.

[62] Skadeståndslag (1972:207).

[63] This development is analysed within different legal areas and discussed in depth in Chamberlain, *Integritet och skadestånd* (Iustus 2020). A main explanation for the traditionally low status of privacy in Swedish law can be found in its tense relationship to the central Swedish principles of freedom of press, freedom of expression and access to public documents. Two important cases where Sweden was found to be in breach of Article 8 ECHR are *Segerstedt-Wiberg and others v. Sweden* (appl. no 62332/00, 6 June 2006) and *Söderman v. Sweden* (appl. no 5786/08, 12 November 2013). These judgments led the legislator to take concrete measures with the aim of enhancing the protection of privacy in Swedish law and fulfilling the obligations of Article 8 ECHR.

[64] Brottsbalken (1962:700).

niary harm. Although it is always challenging to keep up with technology and new forms of privacy invasions, today we thus have a relatively solid protection of sensitive information in Swedish tort law – through criminal law.

International law, too, has had a decisive impact on Swedish tort law in this area. Following case law from 2005 onwards, the European Convention of Human Rights (ECHR) has been used as a legal base for awarding compensation regarding non-pecuniary loss – not least its Article 8 on the right to respect for privacy.[65] Since 2018, the case law is codified in Chapter 3, § 4 of the Damages Act. This development where human rights are used as the legal base for damages claims has been groundbreaking in Swedish tort law, and the ECHR cases also paved the way for the possibility to use the fundamental rights in Chapter 2 of the Swedish Instrument of Government[66] in the same way.[67]

On the topic of this chapter, one issue after this short overview of applicable tort law is if for instance unauthorised spreading of sensitive personal information should be addressed within data protection law or within tort law through criminal law (or convention law). According to the general principle of *lex specialis*, Article 82 of the GDPR should be the firsthand choice. However, in Swedish case law the amounts of compensation have so far been higher when a rights-based legal provision is used (such as Article 8 ECHR), or even when criminal law is used (such as spreading of sensitive information, Chapter 4 § 6 a Criminal Code) as base for application of Chapter 2, § 3 of the Damages Act. This means that data protection law is likely not used in a lot of tort law cases where it could be – or used only in combination with other legal bases, in order to achieve higher compensation.[68] This development could give rise to questions regarding the efficiency of EU law in Sweden and the central principle of loyalty that binds the Member States (Article 4 Treaty of the European Union, TEU). It should also be noted that the threshold for damages under Article 82 GDPR appears to be lower than according

[65] See especially case NJA 2007 p. 584.
[66] Regeringsformen (1974:152).
[67] Since 2022, there is a reference also to the Instrument of Government in Chapter 3, § 4 of the Damages Act.
[68] See NJA 2013 p. 1046 (3 000–5 000 SEK is set as the standard compensation for wrongful treatment of personal data); proposition 2000/01:68 p. 65 (minimum amount of damage for non-pecuniary harm resulting from serious violations according to Chapter 2, § 3 of the Damages Act is 5 000 SEK); preparatory work proposition 2017/18:7 p. 66 (minimum amount of compensation for a violation of rights is set to 10 000 SEK). It should be noted that these figures are probably somewhat higher today, at least regarding compensation for data protection breaches and non-pecuniary damages resulting from serious violations. After updates of the Damages Act in 2022, damages according to Chapter 2, § 3 are to be doubled and the minimum level should therefore rise to 10 000 SEK (preparatory work proposition 2021/22:198).

to the Damages Act, with its prerequisite of "serious violation". In the first case from the CJEU interpreting Article 82, it was made clear that – while a mere breach of the regulation in itself cannot be considered to define harm, and a plaintiff thus must show that the breach in question has resulted in actual harm, it goes against EU law for a Member State to demand a certain degree of severity in order for the harm to be compensable.[69]

3.3 The Name and Image Act

Another specialised law that protects personal information is the short law on names and images in commercial practices of 1978.[70] In § 3 of the so-called Name and Image Act, it is stated that fair compensation shall be awarded to persons whose name or image have been used in commercials without their consent (strict liability). If fault or intent has been established in using names or images, compensation for non-pecuniary damage may also be awarded. The protected interest of the regulation can perhaps best be described as the *personality*, but all the same it protects personal information. As with the Swedish Data Act, the early Name and Image Act comes across as progressive with its strict liability and permissive approach to non-pecuniary harm. Case law has not been so extensive, but establishes compensation at higher levels than according to the Swedish Data Act or Damages Act. The explanation for this can be found in the fact that the protected interest of the law is primarily the commercial persona or trademark of individuals, which means that reputational damage is compensable.[71]

3.4 The Product Liability Act?

An interesting development in the intersection between AI and tort law is the current adaptation of the Product liability directive of 1985.[72] In a new version of the directive proposed in 2022,[73] the Commission aims to include digital products and services such as AI based systems in the concept of defective products. Faulty AI products may thus in the near

[69] Case C-300/21, *UI v. Österreichische Post AG*, ECLI:EU:C:2023:370 (judgment of May 4th, 2023).
[70] Lag (1978:800) om namn och bild i reklam.
[71] See NJA 1999 p. 749 (damages of 75 000 SEK).
[72] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. In Sweden the rules can be found in produktansvarslag (1992:18).
[73] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM/2022/495 final.

future lead to product liability – a form of strict liability, with new rules on the disclosure of evidence and burden of proof that are favourable to consumers.[74] The updated directive would cover *material* losses resulting from loss, destruction or corruption of data, according to proposed Articles 4 (6) (b–c) and Article 5.[75] However, according to section 2 of the Explanatory Memorandum, the proposal "does not address other types of harms, such as privacy or discrimination, which would be more appropriately dealt with under other legislation". As Li has concluded, this means that the issue of non-material harm is left to the Member States – if it is not considered covered by the GDPR.[76] Here we thus have a potential gap between EU regulations, where classic tort law may have to step in to cover damages resulting from violations of fundamental rights such as privacy.[77]

4. Data protection and the proposed regulation on artificial intelligence

Apart from the above existing – and proposed – consumer law and tort law legislation and their contribution to data protection, we would also like to bring to the fore some proposed EU laws that are more difficult to categorise as consumer or tort law related, but instead aim mainly at regulating AI[78] and the contemporary digital environment. The reason for looking into these laws is that they fall into the same category as the ones above, namely legislation that adds to the field of data protection. The AI development easily sparks concern regarding data processing, as AI systems function better the more data they are trained on. How are

[74] See Articles 8–9 of the proposed Directive. Similar alleviations are put forth in the Commission's proposed AI Liability Directive (Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, COM/2022/496 final). This legal act is intended to harmonise procedural rules, making it easier for victims regarding the burden of proof in cases of fault-based liability where AI is involved.

[75] For a comprehensive analysis of the proposal, see Wagner, 'Liability Rules for the Digital Age', 2022, 13 Journal of European Tort Law 3, pp. 191–243. Wagner describes the inclusion of data into the scope of protection as a "welcome acknowledgment of the changing landscape of property in the digital era" (ibid p. 211).

[76] Li, 'Risk regulation and tort damage in the era of AI: Status quo and gaps' (https://blog.ai-laws.org/risk-regulation-and-tort-damage-in-the-era-of-ai-status-quo-and-gaps/), 29 January 2023. See also, on the topic of AI liability, Li, Faure & Havu, 'Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach', 2022, European Journal of Risk Regulation 13, pp. 618–634.

[77] It may be mentioned that also other legal areas that are not in focus in this contribution have been important for the Swedish development of legal protection for personal information; for instance register laws, camera surveillance laws, libel and secrecy rules.

[78] The version used here is the European Commission's proposal of April 2021.

the two comprehensive regulations of these two areas – the GDPR and the AI Act – to relate?

Even though the AI Act claims that it is without prejudice to the GDPR, it is rather apparent that the AI Act and the GDPR are both applicable in parallel, the AI Act "complementing" the GDPR.[79] The question is what this means more specifically. While the GDPR is mentioned only once, in the context just described, the term "data protection" appears 30 times in the AI Act. Under the heading "Prohibited Artificial Intelligence Practices", some *manipulative practices* constitute prohibited practices under the AI Act.[80] As we argued above, manipulative practices, such as dark patterns, are also addressed by consumer protection legislation. However, the AI Act builds upon this understanding of prohibited practices and clarifies that some specific practices, the ones using subliminal techniques, which are often based on the personal attributes of individuals, should always be regarded as prohibited since the risks arising from such a use of AI are considered to be unacceptable.

The AI Act in general is built around AI systems of different risk levels. The motivation for prohibiting systems with "unacceptable risks" is that the use of them is considered "contravening Union values, for instance by violating human rights"[81]. "High-risk" systems are permitted but heavily regulated, as they "create a high risk to the health and safety or fundamental rights of natural persons".[82] The proposal even specifically mentions the right to data protection and privacy in relation to these categorisations.[83] However, and even more importantly, the proposal gives a clear picture of what the legislator understands as important and less important risks to the fundamental rights of individuals.

This elaboration on risk and risk assessments could potentially be of use also for the area of data protection. The GDPR too is a risk-based regulation, in the sense that the legislator has put an obligation on data controllers to assess the risks arising when they process personal data and mitigate or eliminate such risks.[84] However, this risk assessment is left upon the data controllers, something that has been regarded as a rather difficult and vague task.[85] The AI Act proposal, thus, could be

[79] AI Act Proposal, Explanatory Memorandum para. 1.2.
[80] AI Act Proposal, Explanatory Memorandum para. 5.2.2.
[81] AI Act Proposal, Explanatory Memorandum para. 5.2.2.
[82] AI Act Proposal, Explanatory Memorandum para. 5.2.3.
[83] AI Act Proposal, Preamble para. 15; 36. See also Preamble, para. 45, on "privacy-preserving" techniques when data sets are used for the development of high-risk systems.
[84] See in depth on this topic Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).
[85] Ferra and others, 'Challenges in Assessing Privacy Impact: Tales from the Front Lines', 2020, 3 Security and Privacy (https://onlinelibrary.wiley.com/doi/10.1002/spy2.101) accessed 14 June 2023.

used exactly in order to help with this assessment by pre-defining situations where some risks are either unacceptable or of such importance that specific precautions must be taken by data controllers.

Related to the risk assessment discussion, it is also worth mentioning here that there is some additional legislation within the Digital Decade Strategy on cybersecurity, which in combination with the proposed AI Act can be used as a tool to help us interpret the GDPR. More specifically, the GDPR has alleviated security as one of its main principles in Article 5(1)(f) and has specified the requirements of security in Articles 25 and 32 on data protection by design and by default as well as on security. In both these articles we find that data controllers should take into consideration the "state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". As it is right now, even though there are a number of decisions by data protection authorities, the CJEU has not ruled on how these two provisions and their requirements should be understood.[86] However, the proposed AI Act and Cyber Resilience Act seem to recognise some of the findings of these authorities and thus concretise how to interpret these provisions.

One of the most important requirements when it comes to assessing whether controllers have implemented appropriate technical and organisational measures in order to protect personal data processing through secure environments, is the assessment of the risks of varying likelihood and severity for the rights and freedoms of natural persons. As we already pointed out, assessing risks has been the main regulatory technique under the GDPR[87] and, consequently, what data controllers have been struggling with. Even though this issue is not easy to crack, the new proposals nevertheless provide some helpful insights on what the EU legislator has understood as high-risk systems. The AI Act has systematised the different risks in four different groups while the Cyber Resilience Act has also defined what products are to be considered as highly risky or critical.[88] The proposal in the Cyber Resilience Act clari-

[86] See however an interesting report from Future of Privacy Forum, 'Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR', May 2023 (https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf), offering an overview of national decisions.

[87] See again Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).

[88] On the relationship between the Cyber Resilience Act and the AI Act regarding products with AI elements, see the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454 final.

fies that one of the goals of this piece of legislation is exactly the security of personal data.

Additionally, and in order to address these risks, the Cyber Resilience Act poses specific obligations on traders related to cybersecurity which seem to provide for a minimum of what cybersecurity should contain. In Annex I we find for example that traders should have knowledge of existing vulnerabilities – and therefore actively monitor for new vulnerabilities[89] – that security should be in place as a default configuration (in the mantra of Security by Default as the Data Protection by Default), that attack surfaces should be limited and so on.

Coming back to the proposed AI Act, another issue that it aims to clarify is related to the massive amount of data that is normally required for the development of AI systems. Article 10 of the AI Act Proposal is entitled "Data and data governance". It regulates high-risk AI systems' use of training on data models and states that training, validation and testing data sets shall be subject to appropriate data governance and data management practices. Amongst these practices, the collection of data is listed. Leaning on Article 10.5, providers of high-risk AI systems may – when strictly necessary to ensure bias monitoring, detection and corrections – process also special categories of personal data as defined in Article 9 GDPR.[90] The condition for this is that appropriate safeguards are applied, for example "privacy-preserving" measures such as pseudonymisation or encryption. According to its Preamble,[91] the AI Act will not provide any separate legal bases for treating special categories of personal data – instead, the legal base will be "substantial public interest" in line with Article 9.2 (g).[92] In this sense, the AI Act will thus not be broadening but instead *developing* the GDPR, or more specifically the rules on using certain data.

As Colonna also argues in her contribution in this anthology, the proposed AI Act adds to the general data protection framework in an additional way, by specifying and broadening the principle of data protection by design. Specifically, the AI Act poses a direct obligation

[89] Information Commissioner Officer, Ticketmaster UK Limited [2020] COM0759008, where the ICO found that the state of the art requirement "includes knowledge, actual and constructive, of attack vectors (i.e. pathways to a target or the methods used by an attacker to compromise a target) current at the date of the Personal Data Breach and whether the measures in response to those attacks are adequate in line with the state of current technologies".

[90] Article 10 of the AI Act Proposal also refers to special categories of data according to Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725.

[91] AI Act Proposal, Preamble para. 41; 44.

[92] Article 9.2 (g) reads: "[…] substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

for human oversight by design, something that can be seen as part of the GDPR's data protection by design requirement. At the same time this design requirement impacts not only the data controllers but "it imposes [this] legal responsibility on downstream actors to implement technical strategies to safeguard the fundamental right of data protection into their systems from the outset of their development, even if this obligation is limited to only providers of high-risk AI".[93]

Lastly, regarding supervision, the European Data Protection Supervisor (EDPS) will be supervising the Union institutions and bodies when they fall within the scope of the AI Act,[94] thus affirming the close connection between data protection and the regulation of AI. Further, where the provisions on prohibited AI practices concern biometric systems with processing of personal data, the legal base for the regulation will be Article 16 Treaty on the Functioning of the European Union (TFEU)[95] – the same legal base as the GDPR.[96] When personal data is processed within the suggested innovative AI systems or "regulatory sandboxes", national data protection authorities should be involved in the process.[97]

5. Conclusions

EU law is becoming more complex, at an ever accelerating pace. This goes not least for the legal area of data protection, which is gaining increasing importance both in the EU and at a global level. As we have seen above, the legal status of data protection is in no way "fixed" with the GDPR; instead, this legal instrument can be seen as a starting point for a more dynamic development. Today, multiple legal acts relating to the handling of data have been decided on or are being negotiated in the EU. This means that the data protection area is spreading and, in this process, creating boundaries, parallels and connections with a striking number of other legal areas.

In this contribution, we have focused on just three examples of interaction between data protection law and other legal areas; namely consumer law, tort law and AI law. We found that there are important tools for data protection embedded in all of the examined areas, both

[93] Colonna, 'Exploring the Relationship between Article 22 of the GDPR and Article 14 of the AI Act' in Westman et al., *Dataskyddet 50 år*.
[94] AI Act Proposal, Explanatory Memorandum para. 5.2.6. The EDPS will also be competent to impose administrative fines on these bodies, see Article 72.
[95] AI Act Proposal, Preamble para. 2. Article 16 TFEU expresses the right to protection of personal data and states that the European Parliament and Council shall lay down rules relating to data protection.
[96] GDPR, Preamble para. 1.
[97] AI Act Proposal, Article 53.

historically and from a contemporary and future-oriented perspective. In consumer law, they can be found in themes such as 1) obligations on providing information regarding processing and security of personal data, 2) obligations to refrain from certain actions, in the sense of commercial practices related to the processing of personal data, and 3) obligations to act in a specific manner, mostly so that personal data are processed in secure environments. Within tort law – a legal area that still differs between Member States, and therefore the Swedish example was used here – data protection mechanisms appear in the Damages Act, the Name and Image Act and the Product Liability Act. The latter is currently being updated at EU level, which is predicted to result in a stronger protection for personal data (but not necessarily privacy). It is also notable that the Swedish Data Act of 1973, which is the object of honour for this anthology, held an impressively progressive clause on damages for wrongful treatment of personal data built on the very same principles as today's Article 82 of the GDPR on damages. Lastly, the budding AI regulation also has the potential to strengthen data protection, for instance through clarifying key concepts such as manipulative practices, security and risk assessments in the context of handling personal data.

Our findings suggest that data protection benefits from the rapid developments of connecting legal areas. However, as things stand it is also important to pause from time to time and ask the sometimes controversial question: Which additional legal provisions and acts are actually needed, and which may primarily create overlaps and confusion? Difficulties to overview and understand a legal field do not strengthen any area or protected interest. Considering this and the fact that the web of legal instruments concerning data protection has never been more complex than today, transparency should be a key concept not just in the ongoing AI debate but also when it comes to designing and developing legal structures such as regarding data protection.