This is the Author's Accepted Manuscript (AAM) version. The final version of the article is published in the Revue européenne de droit de la consommation/European Journal of Consumer Law (2024/1).

"A SPECIAL OFFER FOR YOU!" – PERSONALISATION OF IN-GAME COMMERCIAL PRACTICES AT THE CROSSROADS OF DATA PROTECTION AND CONSUMER PROTECTION REGULATION

Pieterjan Declerck[1], Eva Lievens[2] & Valerie Verdoodt[3ϕ]

ABSTRACT

The videogame industry has exponentially grown in recent years, both in terms of generated revenue and numbers of players around the world. Data-driven videogame business models increasingly rely on both micro-transactions and the monetisation of personal data provided by players. These evolutions have led to personalisation of commercial practices within videogames based on player data. Such personalisation practices may be used to encourage players to spend more time and money on videogames by targeting them with in-game personalised advertising, offers for purchases and prices. Personalisation for commercial purposes raises important questions about the rights of players, who assume dual roles as consumers and data subjects. This article aims to investigate the limits of lawfulness for personalisation of commercial practices from a dual perspective, delving into common concepts of consumer and data protection law – fairness, transparency and vulnerability – with a specific focus on young players. It explores in particular how rules laid down in the General Data Protection Regulation and the Unfair Commercial Practices Directive apply and interact to ensure player protection.

KEYWORDS

Consumer protection; Data protection; Personalisation; Videogames; Children

[1] Pieterjan Declerck is a doctoral researcher at the Faculty of Law and Criminology, Research Group Law & Technology at Ghent University, Belgium.
[2] Eva Lievens is Professor of Law & Technology at the Faculty of Law and Criminology, Ghent University, Belgium.
[3] Valerie Verdoodt is a postdoctoral research fellow at the Faculty of Law and Criminology, Research Group Law & Technology at Ghent University, Belgium.
[ϕ] The authors are affiliated to the FWO-SBO Gam(e)(a)ble research project, which focuses on the blurring lines between videogaming and gambling and its impacts on young people (grant number: S006821N / FWO.SB02020001301). The project's website can be accessed via <https://www.gameable.info/>.

I. INTRODUCTION

Nowadays, videogames are immensely popular among both adults and children. Market research shows that with each younger generation, videogaming engagement increases, forecasting a surge in player numbers around the world to an impressive 3.1 billion by the close of 2027.[4] Concurrently, the videogaming market experiences exponential growth, with projections envisioning its value soaring to 321 billion US dollars by 2026.[5] This remarkable trajectory is driven by pivotal shifts within the videogaming industry. First, there has been a noteworthy shift towards the adoption of a microtransaction model, revolutionising the revenue structure of games.[6] The shift is characterised by smaller, ongoing payments as opposed to traditional one-time transactions, reshaping the financial dynamics of the industry. Second, a distinct trend has emerged towards more data-driven business models in gaming.[7] Videogames are a prime example of digital content and services[8] wherein consumers not only or always pay with money, but also generate valuable personal data that can be monetised. Consequently, this evolution has led to the personalisation of in-game content, including in-game advertising and purchases. The personalisation of in-game commercial practices raises important questions about the rights of players, who assume dual roles as consumers and data subjects. This issue requires scrutiny from the perspective of both consumer and data protection law.

Consumer protection law and data protection law are both crucial legal areas for today's digital society. The former mainly focuses on protecting consumers in their relations with traders, the latter predominantly aims to ensure fair processing and collecting of personal data. Both sets of rules, aiming to achieve fundamental values of the European Union,[9] are increasingly converging in our data-driven economy, in which data is gathered and exchanged between different economic actors to create value. Consumers in the digital environment nowadays frequently encounter goods and services in the context of which collected consumer data is monetised, and services are personalised on the basis of that personal data.[10] The adoption of

---

[4] J. Clement, "Global Video Game Users 2027", 2023, <https://www.statista.com/statistics/748044/number-video-gamers-world/>.

[5] S. Read, "Gaming Is Booming and Is Expected to Keep Growing. This Chart Tells You All You Need to Know.", 2022, <https://www.weforum.org/agenda/2022/07/gaming-pandemic-lockdowns-pwc-growth/>.

[6] Newzoo, "Global Games Market Report 2023", 2023, <https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2023-free-version>; The Business Research Company, "Online Microtransaction Global Market Report", 2023, <https://www.thebusinessresearchcompany.com/report/online-microtransaction-global-market-report>.

[7] T. Crepax and J. T. Muehlberg, "Upgrading the Protection of Children from Manipulative and Addictive Strategies in Online Games: Legal and Technical Solutions beyond Privacy Regulation", *31 The International Review of Information Ethics*, 2022.

[8] European Commission (2021) Commission Notice Guidance 2021/C on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (OJ 2021, C 525/01, p. 1) at p. 11: "*Downloadable games would normally qualify as online* digital content *when their use does not depend on continuous involvement of the game supplier. In contrast, online games provided in a cloud environment would qualify as* digital services*. In-game micro-transactions (in-app purchases) in such games that enhance the playing experience of the respective user, such as virtual items, would normally qualify as contracts for online* digital content*. Also in-app purchases of content that could be used outside the game (e.g. a recording of the gaming session that can be downloaded or shared on a video-sharing platform) would normally constitute a contract for online* digital content*. In contrast, the purchase of premium content that expands the online gaming environment would represent a new* digital service *that complements the original one*" (emphasis by the authors).

[9] The right to data protection is seen as a fundamental right under Article 8 Charter of Fundamental Rights of the European Union (CFREU) and referred to in Article 16 Treaty on the Functioning of the European Union (TFEU), whereas the importance of a high level of consumer protection is highlighted in Article 38 CFREU and Articles 12, 114(3) and 169 TFEU.

[10] N. Helberger, F. Borgesius and A. Reyna, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *54(5) Common Market Law Review*, 2017.

such data-driven business models has led to a simultaneous application of both consumer protection and data protection rules at the level of the European Union.[11] Services, such as video-sharing platform services, social media or online videogames, may be subject to the rules of both frameworks: the General Data Protection Regulation (GDPR)[12] for data protection aspects and consumer protection instruments, such as the Unfair Commercial Practices Directive (UCPD),[13] for consumer protection aspects.[14] Recently, the Court of Justice of the European Union (CJEU) has noted as well that one commercial practice can be an infringement of both frameworks in the recent *Meta* case.[15] In addition, recent legislative instruments, such as the Digital Content and Services Directive (DCSD)[16] and the Digital Services Act (DSA)[17] have imposed specific rules for digital content and services and the platforms that make them available, while acknowledging the importance of public policy objectives in relation to data protection and consumer protection.[18]

This article aims to investigate the lawfulness of personalisation of in-game advertisements and purchases under the above-mentioned legal instruments. The research adopts a dual perspective, delving into the application of both consumer and data protection laws, providing insights into these increasingly closely linked frameworks offering players protection. In the first part, the phenomenon of personalisation of in-game commercial practices is elucidated, including which types of personalisation exist, which monetisation techniques are used, and which types of data are or could be used to personalise offers in videogames. The second part explores synergies between consumer and data protection law by discussing three common underlying concepts – fairness, transparency, or vulnerability – and how these can contribute to the protection of (young) players in the videogame context. Recent research has shown that

[11] V. Verdoodt, E. Lievens, E and A. Chatzinikolaou, "The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?", *Media and Communication, 11(4)*, 2023.

[12] 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 (hereinafter 'General Data Protection Regulation'). Additionally, the ePrivacy Directive might also be applicable. This instrument, however, is not discussed within the scope of this Article.

[13] 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 (hereinafter 'Unfair Commercial Practices Directive').

[14] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 68): "*Data-driven practices involve an interplay between EU data protection legislation and the UCPD".* The Audiovisual Media Services Directive, which is also relevant in the digital environment, especially as its scope was extended to video-sharing platforms, does not cover online games and, hence, falls outside of the scope of the article.

[15] "*The infringement of the rules intended to protect consumers or to combat unfair commercial practices – infringement which a consumer protection association, such as the Federal Union, aims to prevent and penalise, inter alia by recourse to actions for an injunction provided for in the applicable national legislation* – may be related*, as in the present case,* to the infringement of the rules on the protection of personal data *of those consumers*" (emphasis by the authors). CJ, Judgment of 28 April 2022, *Meta Platforms Ireland,* C-319/20, ECLI:EU:C:2022:322, paragraph 67.

[16] 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 (OJ 2019, L 136, p. 1).

[17] 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 (OJ 2022, L 277, p. 1) (hereinafter 'Digital Services Act').

[18] E.g. Recital 48 DCSD, or Recitals 3 and 81 DSA.

a considerable percentage of children in Europe play videogames,[19] and that parents, although aware of existing parental control mechanisms, are concerned about the time and money their children spend on videogames.[20] Finally, the third part of the paper provides a discussion on the legal limits for personalisation in videogames under consumer protection and data protection law – with a focus on the UCPD and GDPR – and highlights key takeaways for future decision-making in this field.

II. PERSONALISATION IN VIDEOGAMES

Monetisation in the videogame environment has changed remarkably throughout the 21st century. Whereas videogames used to be offered as a finished product for which the player pays a price, an evolution has taken place in which videogames are more and more offered as a continuous service or experience for players.[21] Instead of paying a fixed price for the full content package, videogames nowadays often offer additional content which is periodically released and can be purchased by the player through microtransactions.[22] This content comes in many forms: new characters, weapons or other usable in-game items, boosts, virtual currency, additional levels, or cosmetic upgrades.

Different monetisation techniques use different methods of acquiring this content by players. They can, for instance, at regular intervals, purchase virtual content through 'small' payments, either directly with 'real' money, or through purchasing a 'virtual' currency which is then subsequently used to acquire the in-game content. This monetisation technique is commonly referred to as 'microtransactions'.[23] Other examples of monetisation techniques include the DLC-model (downloadable content), where players pay a one-time price to gain access to additional content; the subscription model, in which players pay a monthly price to ensure continuous access to additional content; or the recently rising 'Battle Pass' model, where players purchase a periodic pass which enables them to acquire additional content by playing the game for a specific amount of time.

Different types of videogames may provide (a combination of) different monetisation techniques, depending on their player-base and the importance of acquiring additional content for the gameplay experience. For example, videogames where the core gameplay loop remains the same – mostly found in competitive games in the Massive Online Battle Arena (MOBA) genre (e.g. League of Legends), First-Person Shooter (FPS) genre (e.g. Counter-Strike or Apex

[19] The European Parliament recently acknowledged that "*some game designs used for in-game purchases are manipulative and exploitative by design*" and that videogame companies need to ensure that videogames targeted towards children respect their rights: European Parliament, Resolution of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI)), 2023, p. 21. Note that no additional clarification is provided regarding when a videogame is 'targeted towards children'.

[20] A significant part of the EU videogame population is under the age of 28. See Videogames Europe and European Games Developers Federation, "All about videogames – European Key Facts 2022", 2022, <https://www.videogameseurope.eu/wp-content/uploads/2023/08/Video-Games-Europe_Key-Facts-2022_FINAL.pdf>.

[21] Also referred to as 'Games-as-a-service' (GaaS). See e.g. C.B. Hart, "The Evolution and Social Impact of Video Game Economics", Lexington Books, 2020.

[22] See e.g. M. Davidovici-Nora, "Innovation in business models in the videogame industry: Free-To-Play or the gaming experience as a service" *2(3) The Computer Games Journal 22,* 2013; D. Zendle, R. Meyer and N. Ballou, "The changing face of desktop videogame monetization: An exploration of exposure to loot boxes, pay to win, and cosmetic microtransactions in the most-played *Steam* games of 2010-2019", *15(5) PLoS ONE,* 2020; L. Van Roessel and J. Svelch, "Who Creates Microtransactions: The Production Context of Video Game Monetization", in O. Sotamaa and J. Svelch (eds) *Game Production Studies,* Amsterdam University Press, 2021.

[23] In free-to-play games, where players do not have to pay to play the game, microtransactions are the dominant monetisation technique as they provide the videogame publisher with a source of revenue.

Legends), or Ultimate Team in sports games – monetisation will often revolve around acquiring periodically released content which varies in rarity and may or may not be desired by players (e.g. new skins for champions in League of Legends, new skins for weapons in Counter-Strike, new player cards in Ultimate Team). In other games (e.g. mobile strategy games such as Clash of Clans or single-player games such as Candy Crush) the offered content may focus more on providing players with an opportunity to acquire additional resources or boosts which they then may or may not use to gain an advantage over other players. Of course, other types of games exist which offer different types of content obtainable by players either for free or through purchase.

This shift in videogame monetisation is clearly highly lucrative. For example, the total revenue generated by the videogame industry was estimated at over 150 billion USD in 2022,[24] and more specifically the global microtransaction market is valued at over 70 billion USD in 2023.[25] Aside from money that is spent on microtransactions, economic value can also be generated by the collection, processing and sharing of personal data of videogame players. Examples of such activities include collecting personal data during the registration process to offer services; the sharing of data between videogame companies and third parties such as social networking sites; or constructing profiles of players to personalise or customise (the price of) offered products or services[26], as well as to influence the decision-making of players. In the mobile videogames industry, in particular, where the free-to-play business model is widely applied,[27] the collection and processing of player data acts as a substitute for money.

To customise players' gameplay experience, large amounts of (personal) data on the player needs to be collected and analysed. For personalisation, the different types of data that are used are usually categorised as 'data that is *provided* by the data subject', 'data that is *observed* about the data subject', and 'data that is *inferred*' or created by the controller on the basis of the two former categories.[28] Such data collection – sometimes also referred to as 'data surveillance' – has become the standard practice in contemporary videogames which deploy one of the business models described above.[29]

Various types of data are gathered, many of which are also mentioned in the videogame companies' terms of use and/or privacy policies: user information (e.g. name, age, gender), commercial information (e.g. order information, payments, subscriptions), communication information, geo(location) data, personal identifiers, technical information about the device or software used in the service, information and statistics about user interactions with the services (including URLs of visited websites, time spent on websites, generated clicks), general

[24] Statista Market Insights, "Games – Worldwide", 2022, <https://www.statista.com/outlook/dmo/app/games/worldwide>.

[25] The Business Research Company, "Online Microtransaction Global Market Report 2023", 2023, <https://www.reportlinker.com/p06246501/Online-Microtransaction-Global-Market-Report.html>.

[26] Data can be sold to data brokers, who specialise in predicting consumers' behaviour using large databases of publicly and privately collected data.

[27] See K. Alha, "The Rise of Free-to-Play: How the revenue model changed games and playing", Tampere University, 2020.

[28] European Data Protection Board (2021) Guidelines 8/2020 on the targeting of social media users, p. 13-14 (emphasis by the authors).

[29] A. Drachen et al., "Game Data Mining" in M. El-Nasr, A. Drachen and A. Canossa (eds*) "Game Analytics: Maximizing the Value of Player Data"*, Springer, 2013; J. Svelch, "Normalizing player surveillance through video game infographics", *New Media & Society 1*, 2022; for mobile games specifically, see M. Bonenfant, A. Dumon and L. St-Martin, "Being played in everyday life: Massive data collection on mobile games as part of ludocapitalist surveillance dispositive" in L. Samuelsson, C. Cocq, S. Gelfgren and J. Enbom (eds), *Everyday life in the culture of surveillance",* Nordicom, 2023 and J. Reynolds, "Gambling on Big Data: Designing Risk in Social Casino Games", *10(1) European Journal of Risk Regulation 116*, 2019.

gameplay data (how players play the game, how much they spend playing, when they will stop playing, what they will or won't do while playing, adapt gameplay to player performance...), or data related to how players feel (e.g. inferences based on emotional analytics).[30] By relying on a concept generally referred to as 'game telemetry', videogame companies can collect gameplay data to improve the gameplay experience for players.[31] For example, the gameplay experience of a player can be personalised through analysis of that player's preferences (gameplay aspects that the player finds appealing), performance (the player's progression and obstacles encountered), in-game behaviour (what actions the player makes) or personality (how the player can be distinguished within the database).[32]

In some cases, the personalisation of the gameplay experience may converge or interact with the personalisation of the monetisation aspects of the videogame. Both forms of personalisation serve the same purpose: to tailor the content to players' individual characteristics and preferences, increasing engagement or in-game purchases, and ultimately maximising profits. Examples of where such forms of personalisation converge include personalised prices for in-game purchases, personalised 'special offers' of in-game items based on players' data profiles, personalised in-game items advertised in the in-game store, or personalised odds in games where randomised reward mechanics are used.

A lack of transparency regarding the algorithms responsible for the personalisation makes it difficult to assess the extent to which personalisation techniques are currently being used in videogames for commercial purposes. The available evidence is limited; while some research contends that achieving true personalisation of content in games necessitates further technological advancements,[33] other studies reveal that patented videogame systems already use behavioural tracking data to optimise purchasing offers.[34] Additionally, players perceive videogame monetisation strategies as nudging them towards making purchases.[35] Regardless of its prevalence and the benefits that personalisation may offer players in terms of relevance

[30] See e.g. Activision's Privacy Policy at 3, <https://www.activision.com/legal/privacy-policy#toc3>; Electronic Arts' Privacy Policy at 1, <https://www.ea.com/legal/privacy-and-cookie-policy?isLocalized=true&setLocale=en-gb> or Blizzard's Privacy Policy at 2, <https://www.blizzard.com/en-us/legal/8c41e7e6-0b61-42c4-a674-c91d8e8d68d3/blizzard-entertainment-privacy-policy#1650658228>.

[31] Telemetrics refers to data about what happens between the player and the videogame, for example purchasing behaviour, physical movement, interactions with the game or with other users. See A. Drachen, M. El-Nasr and A. Canossa, "Game Analytics - The Basics" in M. El-Nasr, A. Drachen and A. Canossa (eds), *Game Analytics: Maximizing the Value of Player Data,* Springer, 2013.

[32] S. Karpinskyj, F. Zambetta and L. Cavedon, "Video game personalisation techniques: A comprehensive survey", *5 Entertainment Computing 211*, 2014.

[33] Zhu and Ontanun mention that this is due to a number of reasons: people play games for a broader range of reasons (challenge, exploration, social activity, etc.), making it more difficult to identify individual player needs and preferences; computer games tend to involve more complex content and user interaction than for instance websites. J. Zhu and S. Ontañón, "Player-Centered AI for Automatic Game Personalization: Open Problems", *arXiv 2102:07548*, 2021, <http://arxiv.org/abs/2102.07548>.

[34] D. King, P. Delfabbro, S. Gainsbury, M. Dreier, N. Greer and J. Billieux, "Unfair play? Video games as exploitative monetized services: An examination of game patents from a consumer protection perspective", *101 Computers in Human Behavior 131*, 2019; K. Sigmon, "Pay to Play: Video Game Monetization Patents and the Doctrine of Moral Utility", *5 Georgetown Law Technology Review 72*, 2021.

[35] E. Gibson, M. Griffiths, F. Calado and A. Harris, "Videogame player experiences with micro-transactions: An interpretative phenomenological analysis" *145 Computers in Human Behavior 107766,* 2023*;* E. Petrovskaya, S. Deterding and D. Zendle, "Prevalence and Salience of Problematic Microtransactions in Top-Grossing Mobile and PC Games: A Content Analysis of User Reviews" *CHI Conference on Human Factors in Computing Systems,* 2022, retrieved from <https://doi.org/10.1145/3491102.3502056>.

and appeal,[36] this paper aims to explore the limits of lawfulness of personalisation of in-game commercial practices from a consumer-data protection perspective.

III. EXPLORING COMMON CONCEPTS ACROSS CONSUMER AND DATA PROTECTION: FAIRNESS, TRANSPARENCY AND VULNERABILITY

As established earlier, both the consumer protection and data protection legal frameworks are relevant to personalisation of in-game commercial practices.

The UCPD defines which commercial practices are considered unfair, and hence, prohibited in the European Union.The 2021 Commission Notice Guidance on the interpretation and application of the UCPD confirms that the UCPD applies to data-driven personalisation practices in the business-to-consumer relationship, including personalisation of advertising and pricing.[37] If such practices are considered to breach the trader's professional diligence requirements (Article 5 UCPD; the 'safety net' for practices that are not caught by other UCPD provisions),[38] amount to a misleading practice (Articles 6-7 UCPD) or an aggressive practice (Articles 8-9 UCPD) or fall within the scope of the blacklisted practices (Annex), they are prohibited.

At the same time, as profiles are constructed from large amounts of personal data collected from the player or obtained from data brokers or third parties such as social media platforms for personalisation purposes, the GDPR must be complied with.[39] The GDPR lays down cornerstone principles that processing activities need to observe (Article 5 GDPR), attributes data subject rights to individuals whose data is processed (such as the right to information – Article 12-14 GDPR – and the right not to be subject to solely automated decision-making when this has a legal or similarly significant effect – Article 22 GDPR) and imposes obligations on data controllers.

Interestingly, the instruments within both the consumer and data protection law framework are underpinned by common key concepts: fairness, transparency and vulnerability. In this section, these concepts are introduced and discussed from the perspective of both domains. The next section then elaborates on their application to the personalisation of in-game commercial practices.

A. – Fairness

Fairness is one of the data protection principles that data controllers must abide by whenever they are processing personal data.[40] The European Data Protection Board (EDPB) has clarified that fairness is "*an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or*

[36] E.g. to enhance the player's gameplay experience based on their preferences, or in educational games (serious games) to offer personalised learning modules.

[37] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 1).

[38] Ibid., p. 37. This may include, for instance, a breach of principles derived from national and international standards and codes of conduct (Ibid., p. 76).

[39] This article does not aim to offer a comprehensive overview of all GDPR obligations that must be respected when processing personal data but focusses on aspects that are of particular relevance to the personalisation of in-game purchases, and the interplay with consumer protection law.

[40] Article 5.1.a: "*Personal data shall be […] processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*".

misleading to the data subject".[41] The potential unfairness of a practice may thus be related to risks for data subjects, including manipulation of users, for instance, when the targeting[42] of a specific message to (a) specific (group of) users is used to influence the behaviour and choices of individuals in a way that undermines their individual autonomy and freedom to decide whether and how their personal data is processed.[43] Examples that are given in that regard include the delivery of "*individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns*".[44] In its 2023 decision regarding TikTok, the Irish Data Protection Commission (DPC) refers to the clarification by the EDPB that in relation to fairness, elements such as the autonomy and expectations of data subjects, avoidance of deception, the power (im)balance between data subjects and data controllers, and truthful processing are important.[45]

The concept of fairness is equally important in consumer protection law. More specifically, the specific objective of several Directives is the protection of consumers against *unfair* interactions with traders. Examples are the protection against unfair commercial practices (UCPD) or against unfair contract terms (Unfair Contract Terms Directive).[46] While there is also no clear definition of the concept of fairness in this context, notions that are associated with it are diligence, honesty or good faith. When the UCPD was proposed, the Commission stated explicitly that greater legal certainty could be achieved by defining unfairness rather than fairness.[47] This unfairness is expressed in the safety net provision, the provision on misleading and aggressive practices and the blacklist (*supra*). The underlying idea is that traders cannot act in a dishonest way, mislead consumers or exploit their 'position of power' vis-à-vis the consumer.[48] In that regard, just as is the case under data protection law, an important aim is to protect the autonomy of the consumer to take transactional decisions.[49] The data-driven economy has caused a significant increase in the importance of fairness in the digital environment, illustrated for example by the potential of digital interfaces to mislead consumers due to their design.[50] As a part of the New Consumer Agenda, the European Commission is performing a fitness check on digital fairness to analyse whether additional action is required.[51] In the videogame environment, the Commission Notice on the UCPD refers *inter alia* to potentially unfair practices regarding in-game purchases and in-game advertisements, and data-

[41] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0), 2020, p. 17–18.

[42] "*Targeting services make it possible for natural or legal persons ("targeters") to communicate specific messages to the users of social media in order to advance commercial, political, or other interests*"; European Data Protection Board (2021) Guidelines 8/2020 on the targeting of social media users, p. 4.

[43] Ibid., p. 7. See also recital 7 GDPR: "*Natural persons should have control over their own personal data*".

[44] Ibid.

[45] See European Data Protection Board, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), p. 22.

[46] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, amended by Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019, (OJ 1993, L 95, p. 29).

[47] European Commission, Proposal for a Directive of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the Internal Market and amending directives 84/450/EEC, 97/7/EC and 98/27/EC (the Unfair Commercial Practices Directive), COM(2003)356 final, p. 7.

[48] C. Willett, "Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive", *33 Journal of Consumer Policy* 33 247–273, 2010.

[49] N. Helberger, F. Borgesius and A. Reyna, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *54(5) Common Market Law Review*, 2017, p. 1455.

[50] BEUC, "Dark Patterns" and the EU Consumer Law Acquis: Recommendations for better enforcement and reform, 2023, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf>.

[51] See European Commission, "Digital fairness – fitness check on EU consumer law", <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en>.

driven personalisation.[52] Moreover, the document explicitly acknowledges the interplay between consumer and data protection law regarding fairness by stating that "*privacy and data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD, particularly in the situation where the trader processes consumer data in violation of privacy and data protection requirements, i.e. for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications*".[53]

B. – Transparency

In data protection law, transparency is closely linked to fairness.[54] Recital 60 of the GDPR, for instance, states that *"[t]he principles of* fair and transparent *processing require that the data subject be informed of the existence of the processing operation and its purposes*".[55] The rationale is that a data subject must be (made) aware of which personal data are processed by whom and for what purpose. Article 12 GDPR requires data controllers to inform data subjects "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*".[56] This should especially be the case when the information is addressed to a child (who has the right to obtain such information when their personal data is processed)[57]. A significant concern in relation to profiling and personalisation is that these processes are often very opaque and happen 'in the background', often unknown to the user.[58]

Transparency in the consumer protection context is related to the broader existing information obligations, for example in Article 6 of the Consumer Rights Directive (CRD)[59] and Article 6-7 UCPD. The underlying objective is similar: assuring that consumers are adequately informed about their transactions with traders in which they are generally considered the weaker party.[60]

---

[52] European Commission (2021) Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market C/2021/9320, OJ 2021, C 526, p. 103).

[53] Ibid., p. 19.

[54] See also DPC Ireland, "Decision in the matter of TikTok Technology Limited", 2023, <https://edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf>. p. 84.

[55] Emphasis by the authors.

[56] Interestingly, in its guidance document on transparency, the EDPB even refers to the Unfair Contract Terms Directive when interpreting the concept of 'clear and plain language', again demonstrating close links between consumer and data protection law; Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 2018, <https://edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf>, p. 8.

[57] See Data Protection Commission (Ireland), "Fundamentals for a Child-Oriented Approach To Data Processing", 2018, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>: "*Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data*".

[58] European Commission, Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 100).

[59] 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: Article 6 (1) (ea) requires the provision of information regarding the fact that the price was personalised on the basis of automated decision-making.

[60] European Commission, Communication COM/2020/696 from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0696>, p. 18.

If material information needed by the average consumer[61] to take an informed transactional decisionis missing, then a practice could be considered unfair according to the UCPD. In the New Consumer Agenda, transparency obligations are highlighted as an important means to tackle informational asymmetries between online traders and consumers.[62]

C. – Vulnerability

Certain data subjects are considered more vulnerable than others. Recital 38 of the GDPR, for instance, states that children merit "specific protection" with regard to their personal data, as "*they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*". The latter sentence indicates a degree of vulnerability, which is confirmed in a number of guidance documents issued by the EDPB, such as the Guidelines on Data Protection Impact Assessments[63] which classify children explicitly as 'vulnerable' data subjects, or the Guidelines on the targeting of social media users which states that *"[t]he potential adverse impact of targeting may be considerably greater where vulnerable categories of individuals are concerned, such as children*".[64] For adults, this is not as clear, although adults might equally display certain vulnerabilities that can be taken advantage of. The EDPB, for instance, refers to targeting of financially vulnerable persons that are interested in online betting.[65]

According to the Commission Notice on the UCPD, data-driven practices may have "*a more significant effect on vulnerable consumers*". Children, again, are a prime example of a vulnerable group.[66] Yet,, consumer vulnerability is a dynamic concept that has been significantly impacted by the increasing digitisation of society.[67] In the definition of the UCPD on vulnerability, three criteria can be distinguished: (i) it needs to concern a particular group of people, (ii) there is vulnerability due to physical infirmity, age or credulity, and (iii) this vulnerability was foreseeable.[68] However, in light of the changes brought about by the digital transformation, this definition has been subjected to extensive criticism, for example because it is too narrow and does not take into account situational or temporary vulnerability.[69] As

[61] A commercial practice must be evaluated from the perspective of the 'average consumer' who is reasonably well-informed, observant and circumspect. Hence, when a particular practice is aimed at a group of consumers (e.g. children, or the player-base of a videogame), the practice will have to be evaluated from the perspective of the average member of that group. Article 5 UCPD; Recitals 18-19 UCPD. See also K. Purnhagen, "More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?" *8(2) European Journal of Risk Regulation 437*, 2017.
[62] Ibid.
[63] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 2017.
[64] See also DPC Ireland, "Decision in the matter of TikTok Technology Limited", 2023, p. 86: "It is relevant to recall that the personal data at issue related to a particularly vulnerable cohort of data subjects, children".
[65] European Data Protection Board, Guidelines 8/2020 on the targeting of social media users, 2021, p. 7.
[66] European Commission, Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market C/2021/9320, OJ 2021, C 526, p. 36.
[67] OECD, Consumer vulnerability in the digital age, 2023, <https://www.oecd-ilibrary.org/docserver/4d013cc5-en.pdf?expires=1698309562&id=id&accname=guest&checksum=B0C01C719E98DEBE147D7398F6022E65>.
[68] Article 5(3) UCPD.
[69] N. Helberger, M. Sax, J. Strycharz and H. Micklitz, "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability", *45 Journal of Consumer Policy 175*, 2022; C. Riefa, "Protecting Vulnerable Consumers in the Digital Single Market", *33 European Business Law Review 612*, 2022; P. Hacker, "Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law", *European Law Journal*, 2021; P. Cartwright, "Understanding and protecting vulnerable financial consumers" *38 Journal of Consumer Policy 119*, 2014; European Parliament, Briefing on Vulnerable Consumers,

highlighted in the New Consumer Agenda, indeed, vulnerability can also be driven by social circumstances or because of particular characteristics of individual consumers or groups of consumers, such as their age, gender, health, digital literacy, numeracy or financial situation.[70] In that regard, the Commission Notice on the UCDP confirms that the concept of vulnerability should actually be understood as dynamic and situational.[71]

Recent policy documents and scholarship offer further guidance on how to interpret vulnerability in the digital environment, for example by highlighting different types of vulnerability, identifying when and why people can be vulnerable, or how the digital environment requires a different approach to vulnerability due to the complexity of online transactions or informational asymmetries between online traders and consumers. [72] The concept of digital asymmetry is relevant to assess vulnerability.[73] The personalisation of in-game offers based on players' behavioural data relies on the knowledge by traders about their consumers.[74] However, the reverse is not true, as players often know little to nothing about the internal mechanisms underlying the company's marketing strategies. This difference in knowledge (the 'asymmetry') results in a 'weaker' position for the player vis-à-vis the videogame company. This has led for example to the BEUC and the OECD arguing for a form of 'universal state of vulnerability' in the digital environment based on this power imbalance, entailing that every consumer is potentially a vulnerable consumer. [75] In the Commission Notice on the UCDP, vulnerability has been linked to data-driven practices such as profiling, behavioural analysis, or personalisation, applied in B2C interactions. This is especially the case for children, who are seen as particularly susceptible to these practices and whom the European Commission and Parliament have highlighted as vulnerable consumers in the videogame environment.[76]

2021, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI(2021)690619_EN.pdf>; European Commission, Consumer vulnerability across key markets in the European Union, 2016, <https://op.europa.eu/en/publication-detail/-/publication/d1af2b47-9a83-11e6-9bca-01aa75ed71a1/language-en>; OECD, Consumer vulnerability in the digital age, 2023; BEUC, "The Manipulated Consumer, The Vulnerable Citizen - BEUC's response to European Democracy Action Plan", 2020, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-075_the_manipulated_consumer_the_vulnerable_citizen.pdf>; BEUC, EU Consumer Protection 2.0 Structural asymmetries in digital consumer markets, 2021, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf>.

[70] European Commission, Communication from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, 2020, p. 16.

[71] European Commission, Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market C/2021/9320, OJ 2021, C 526, p. 100.

[72] See footnote 62.

[73] BEUC, EU Consumer Protection 2.0 Protecting fairness and consumer choice in a digital economy, 2022, p. 3.

[74] N. Helberger, M. Sax, J. Strycharz and H. Micklitz, "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability", *45 Journal of Consumer Policy 175*, 2022.

[75] BEUC, EU Consumer Protection 2.0 Structural asymmetries in digital consumer markets, 2022; OECD, Consumer vulnerability in the digital age, 2023.

[76] European Commission, Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market C/2021/9320, OJ 2021, C 526, p. 103); European Parliament, Resolution of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI)), 2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023IP0008>, at 13-17.

IV. PERSONALISATION OF IN-GAME COMMERCIAL PRACTICES AT THE CROSSROADS OF CONSUMER AND DATA PROTECTION LAW

A. After having explored three synergetic concepts which are fundamental to both data protection and consumer protection law, the aim of this section is to examine particular legal limits that both frameworks impose on personalisation in videogames, sometimes in parallel, sometimes in a complementary way. A first limit that is addressed is found in the data protection framework, more specifically, in Article 22 GDPR which includes a prohibition ofcertain types of profiling-based decisions. The application of Article 22 GDPR might depend on the qualification of a commercial practice as unfair, and vice versa. Second, limits are imposed through provisions in the GDPR and UCPD that prohibit unfair practices. Third, practices might not comply with both frameworks if there is a lack of information, or if a practice is considered misleading. In assessing the different limits, vulnerability is identified as a recurrent factor. Finally, this section briefly focusses on the challenges related to the enforcement of both frameworks..**Personalisation and Article 22 GDPR**

Starting from the finding that personal data may be collected in the videogame environment to offer personalised commercial offers, a first question that arises concerns the potential application of Article 22 GDPR. According to this provision, data subjects possess the right not to be subjected to a decision (1) based solely on automated processing, including profiling,[77] and (2) which produces legal or similarly significant effects. The Article 29 Working Party (WP29; the predecessor of the EDPB)[78] has emphasised that this right essentially constitutes a prohibition of such processing, unless the controller can rely on one of three exceptions, including the explicit consent of the data subject.[79]

A first condition that needs to be fulfilled for the prohibition to apply is that the decision needs to be 'solely automated'. This entails that "*humans do not exercise any real influence on the outcome of a decision-making process*".[80] While online personalisation can be both solely automated and non-automated, the latter involving human intervention rather than algorithms,[81] within the videogame environment it is hard to imagine that the personalisation of in-game purchases would not be fully algorithmically driven. Considering that existing research has shown certain videogame systems to use behavioural tracking data for the optimisation of purchasing offers (as discussed *supra*), this is likely to fall within the scope of Article 22 GDPR.

---

[77] Article 4 GDPR explains that 'profiling' means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

[78] The Article 29 Working Party was a body at the EU level, which gathered representatives from all EU data protection authorities. They provided guidance regarding the interpretation of the 1995 Data Protection Directive. This body was replaced by the European Data Protection Board under the GDPR. See <https://edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en>.

[79] Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2018.

[80] G. Sartor and F. Lagioia, "The impact of the General Data Protection Regulation on artificial intelligence" (Study commissioned by the European Parliamentary Research Services), 2020, p. 59, retrieved from <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>

[81] Non-automated personalisation of pricing would require direct contact between the trader and the consumer. P. Rott, J. Strycharz, F. Alleweldt, "Personalised Pricing", a Study requested by the IMCO Committee of the European Parliament, 2022, <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/734008/IPOL_STU(2022)734008_EN.pdf>, p.11.

The second condition to assess is whether such personalised in-game purchase offers could be considered to have 'a legal or similarly significant effect'. In this regard, it could be argued that a breach of consumer protection rights could amount to a *legal* effect in the context of Article 22 GDPR. This would mean that if a personalisation practice is considered contrary to professional diligence, misleading or aggressive under the UCDP (*infra*), this practice could also entail the prohibition of Article 22 GDPR.[82] Furthermore, personalisation could in certain situations also be considered to have a '*similarly significant effect*'. This is the case for effects which "*significantly affect the circumstances, behaviour or choices of the individuals concerned, have a prolonged or permanent impact on the data subject, or lead to the exclusion or discrimination of individuals*".[83] Although it has been argued that this condition will not always be fulfilled in case of 'targeted advertising',[84] factors such as the intrusiveness of the profiling process and the use of knowledge regarding vulnerabilities of the individuals involved, could lead to such an effect.[85] The WP29 has stated before that, for instance, targeting financially vulnerable persons might potentially significantly and adversely affect their financial situation, triggering the prohibition of Article 22 GDPR.[86] In the video-game environment, players' vulnerabilities can be known to the videogame companies as a result of their data collection and processing activities, and this knowledge can subsequently be used to increase the chances of these players making purchases in the videogame. This was highlighted by the WP29, stating that profiling can be used to "*target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts*".[87] Such processing practices could thus be prohibited under Article 22 GDPR, unless there is explicit consent from the data subject (or if one of the other exceptions applies). In this regard, the question may be asked whether such consent can be considered valid (in particular, free and informed, *infra*).[88] Yet, even if this would be the case, a practice could still violate the principle of fairness (*infra*).

Additionally, although this is not explicitly mentioned in Article 22 GDPR, the WP29 has stated that organisations should, in general, refrain from profiling *children* for marketing

[82] The same reasoning could be used regarding the AI-based systems that will be prohibited under the upcoming Artificial Intelligence Act, more in particular AI systems that manipulate human behaviour to circumvent their free will and AI used to exploit the vulnerabilities of people (due to their age, disability, social or economic situation); see European Parliament, Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI, 9 December 2023, retrieved from <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>.

[83] WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, p. 21.

[84] G. Sartor and F. Lagioia, "The impact of the General Data Protection Regulation (GPDR) on artificial intelligence" (Study commissioned by the European Parliamentary Research Services), 2020, p. 60.

[85] WP 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, p. 22.

[86] EDPB, Guidelines 8/2020 on the targeting of social media users, 2021, p. 26. In its Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, the WP29 states that "*[i]n many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals*". Yet, it admits that it is possible that it may do so. In that assessment, criteria that can be taken into account are "*the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services; the expectations and wishes of the individuals concerned; the way the advert is delivered; or using knowledge of the vulnerabilities of the data subjects targeted*"; Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018, p. 22.

[87] Ibid., p. 29.

[88] According to Article 4 (11) 'consent' of the data subject means "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

purposes.[89] This is because children are particularly susceptible – or vulnerable – to such practices in the online environment and are more easily influenced by behavioural advertising. Children, it is argued, – depending on their age and maturity – may not have the adequate skills to comprehend the motivation behind this type of marketing or the consequences thereof. Although the WP29 does not go as far as stating that profiling children for commercial purposes is always prohibited, such a prohibition has been advocated for by the UN Committee on the Rights of the Child in its General Comment No. 25 on children's rights in the digital world. There, it is stated that profiling or targeting of children for commercial purposes based on a digital record of their characteristics or based on group data should be prohibited.[90] Most recently, a prohibition of profiling-based advertising has been included in the Digital Services Act (Article 28.2). The prohibition is imposed on 'online platforms'. It has been argued that this might cover videogame environments, depending on their functionalities (for instance, if a game incorporates a system that allows multiplayer communications and where those communications are not a minor or ancillary part of the service; or if a game enables players to create and distribute content within the game; or if a gaming environment contains a type of bulletin board or social media functionality).[91]

Finally, at the same time, not respecting Article 22 GDPR could be considered an unfair commercial practice, keeping in mind the Commission's statement in its Notice that "*privacy and data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD*", referring to processing for commercial purposes like profiling, personal pricing or big data applications.[92]

B. Personalisation and (un)fairness

Shifting our gaze away from Article 22 GDPR, personalisation of in-game commercial practices could in certain instances be considered 'unfair', when obligations applicable to personalisation practices provided for in both the data protection and consumer protection framework are violated. The CJEU has noted on several occasions that the principle of consistency of EU law under Article 7 TFEU endorses a coherent interpretation of notions (such as 'consumer') or provisions in different legal domains.[93] It could be argued that this should also apply to the notion of 'fairness'. As such, Article 5.1.a GDPR on fair data processing could be linked to the concept of 'unfairness' under the UCPD, which could mean for example that a breach of the fair data processing principle may indicate – but not conclusively determine – the unfairness of a commercial practice, just as a practice deemed unfair under UCPD could simultaneously constitute a breach of the Article 5.1.a GDPR.[94] Such an approach is also present in the Opinion of Advocate-General Trstenjak as regards a case where the qualification of a commercial practice as unfair should also be taken into account in

[89] Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2018, p. 29.
[90] United Nations Committee for the Rights of the Child, General Comment 25 on children's rights in relation to the digital environment, 2021, p. 7.
[91] G. Couneson et al., "Gaming Series #2: Online Safety and Gaming – EU and UK Approaches to Regulation", Linklaters Tech Insights, 2023, <https://techinsights.linklaters.com/post/102ig9a/gaming-series-2-online-safety-and-gaming-eu-and-uk-approaches-to-regulation>.
[92] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 19).
[93] CJEU, Case C-694/17, *Pillar Securitisation*, ECLI:EU:C:2019:345, para. 34-35; CJEU, Case C-508/12, *Vapenik*, ECLI:EU:C:2013:790, para. 25.
[94] B. Keirsbilck, "Interaction between Consumer Protection Rules on Unfair Contract Terms and Unfair Commercial Practices", 2013, *50 Common Market Law Review 247,* p. 260.

assessing the (un)fairness of a contractual term: *"[…] a coherent interpretation of the relevant rules of law […] is all the more necessary as the two [regulatory instruments] demonstrate a convergence in the direction they take […] to protect the ability to make judgments and the freedom of choice in business dealings*."[95]

When personalised offers are based on user profiles created using behavioural data, the concept of unfairness becomes particularly relevant when these profiles are used to target players in a way that may be perceived as unexpected, manipulative[96] or exploitative. More specifically, personalised offers may use the information extracted from the data collection practices to nudge users towards making certain decisions. Manipulation or (deceptive) nudging of data subjects has been argued to go against the fairness principle of Article 5.1.a GDPR.[97] In videogames, some examples of commonly used commercial practices are time-limited in-game purchases with limited availability (often limited in time, but sometimes also limited in quantity)[98], using specific sound or visual effects to highlight promotional offers, or pop-up notifications containing offers when encountering an obstacle to in-game progress.

In situations where these offers are personalised based on insights from behavioural data, they could also be seen as unfair under the existing consumer protection framework due to the undue influence that players may experience, for instance to spend more money in the game, amounting to an aggressive commercial practice under Articles 8 and 9 UCPD.[99] More specifically, these offers may be unfair because they exploit players' behavioural biases, based on inferences from collected personal data. For example, a player receives a timed offer for a microtransaction when encountering an in-game obstacle (e.g. the player has to win a battle with their army but fails and subsequently receives an time-limited discounted offer for an army boost). In situations where these offers are tailored to the player's specific characteristics (or even emotional state) on the basis underlying behavioural data and (past) behaviour in the game,[100] they could arguably be seen as unfair when they cause players to take transactional decisions they would otherwise not have made.

Additionally, the European Commission has indicated that the use of information or data about the vulnerabilities of specific consumers (e.g. financial situation, psychological profile, mood) or groups of consumers for commercial purposes, could amount to the exercise of undue influence, and hence, again, be considered an aggressive commercial practice prohibited under Articles 8 and 9 UCPD.[101] In practice, however, establishing proof of the deceptive or manipulative character of personalisation practices might be challenging.[102] In that regard,

[95] AG Trstenjak, Opinion of 29 November 2011, *Perenicova and Perenic,* C-453/10, ECLI:EU:C:2011:788, para. 90.

[96] Note that scholars warn against the use of the notion 'manipulation' as it requires *per definition* intent; N. Helberger, M. Sax, J. Strycharz and H. Micklitz, "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability", *45 Journal of Consumer Policy 175*, 2022; see also P. Hacker, "Manipulation by algorithms: Exploring the triangle of Unfair Commercial Practices, Data Protection, and Privacy Law", 2021, *European Law Journal (forthcoming).*

[97] European Data Protection Board, Guidelines 8/2020 on the targeting of social media users, 2021, p. 4; European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 2022, at 18.

[98] For example, a player can purchase an amount of virtual currency or items at a discount for a period of 24 hours and can repeat this purchase for maximum three times.

[99] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 104).

[100] E.g. offering a lootbox purchase instead of a direct purchase because in the past the player has shown increased purchasing behaviour of lootboxes vis-à-vis direct purchases.

[101] Ibid., p. 100.

[102] OECD, Consumer vulnerability in the digital age, 2023, p. 44.

proposals have suggested a reallocation or reversal of the burden of proof.[103] Specifically in relation to children, personalised advertisements or offers for in-game purchases may in any case not include a 'direct exhortation to buy' (e.g. additional in-game items), as this could qualify as a black-listed, and hence always, unfair practice (Annex UCPD, point 28). This is the case for games targeted at children, but also for games which traders can reasonably foresee to likely be appealing to children, according to the Commission.[104]Finally, if personalisation practices are seen as contrary to professional diligence (which refers to concepts such as honest market practices and good faith, emphasising values that apply in the business environment)[105] and materially distort or are likely to distort the economic behaviour of the average consumer they address, they will be deemed unfair under Article 5 UCPD. In that regard, non-compliance with data protection obligations (e.g. violating data protection principles such as lawfulness, transparency or data minimisation) when personalising commercial practices in videogames could also lead to their qualification as an 'unfair' commercial practice.[106]

C. Personalisation and transparency

Finally, the personalisation of in-game purchases could also lead to transparency concerns. It has been argued that many consumers and data subjects are unaware of personalisation practices.[107] To comply with the legal obligations in place, it must be transparent which personal data is collected for what purposes (Article 12 and 13 GDPR), and how personalisation works (Article 13.2 (f) GDPR). Furthermore, the Commission Notice emphasises that, if the trader does not inform a consumer that the data provided will be used for commercial purposes, this could be considered a misleading omission of material information under Article 7(2) UCPD.[108] A combined approach of data and consumer protection rules may serve as a guideline regarding what threshold of transparency should be expected, or what the standard for information obligations should be.

Recent policy documents at the EU level have hinted at additional requirements regarding informing consumers about in-game content. For example, the EU Parliament has called for more transparency from videogame companies on lootbox[109] probabilities and more fundamentally, on what the algorithms behind the lootboxes are trained to achieve.[110] The European Commission has recently stated that prices of in-game content need to be stated in

[103] BEUC, "Towards European Digital Fairness - BEUC Framing Response Paper For The Refit Consultation", 2023, <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf>, p. 6.
[104] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 105).
[105] Article 2(h) UCPD.
[106] N. Helberger, F. Borgesius and A. Reyna, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *54(5) Common Market Law Review*, 2017, p. 1455.
[107] BEUC, "Automated decision making and Artificial Intelligence - A consumer perspective BEUC Position Paper", 2018, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf>.
[108] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 19).
[109] Lootboxes are virtual items in videogames (often chests) that are either obtained through gameplay or through purchase with real money and provide randomised rewards. See D. Zendle et al., "The prevalence of lootboxes in mobile and desktop games" *115(9) Addiction*, 2020.
[110] European Parliament, Resolution of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI)), 2023, p. 22.

real currency and not only in virtual currency, that the main characteristics of in-game content need to be explained, and that consumers cannot be misled through the use of the word 'free' when in-game purchases are de facto needed to progress in the game.[111] As the videogame environment is an inherently immersive environment where commercial content (e.g. advertising) is often integrated within the gameplay aspects,[112] it may be unclear to users – and vulnerable users, such as children in particular – that the offers they encounter in the videogame are personalised.[113] Both in data protection and consumer protection law, the target group and its vulnerabilities[114] must be considered in providing transparency. Information that is given to children must be understandable from the perspective of an average child.[115] This might require adapting the vocabulary, tone and style of the language, and specific formats such as cartoons, pictograms, animations.[116] As such, according the European Commission, when the commercial element is not sufficiently clear and distinguishable from gameplay, in-game promotions and advertisements could be considered a misleading practice under Articles 6 and 7 UCPD.[117] Finally, it has been argued that transparency is not the silver bullet. The OECD, for instance, posits that "disclosing the personalised nature of a practice is unlikely to be sufficient in isolation as a protective measure".[118] **D. Enforcement**

Our analysis has shown that, while there might be circumstances in which personalisation of in-game purchases is lawful, there are important limits to such data-driven practices both from a data protection perspective (in particular, those laid down in Article 5.1.a Article 12-13, and Article 22 GDPR) and from a consumer protection perspective (in particular, the thresholds for a commercial practice to be classified as unfair, misleading or aggressive, in Article 5-9 UCPD and its Annex).

Yet, an adequate protection of players can only be ensured if both sets of rules are properly enforced by the relevant authorities. Given the synergy between the two fields, efficient enforcement might necessitate cooperation between consumer protection authorities and data protection authorities, for instance regarding the interpretation of common concepts, and the impact of fast technological developments on both fields. At the EU level, the Consumer Protection Cooperation Network exists and is materialised through the CPC-Regulation;[119] whereas national Data Protection Authorities cooperate in the context of the European Data Protection Board.[120] Enforcing data protection and consumer protection rights before a national

[111] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 104-105).
[112] V. Verdoodt, "Children's Rights and Commercial Communication in the Digital Era. Vol. 10.", Intersentia, 2020.
[113] BEUC, "Automated decision making and Artificial Intelligence - A consumer perspective BEUC Position Paper", 2018.
[114] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 2018, retrieved from <https://edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf, p. 11>.
[115] Ibid., p. 7; Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 34 and 100).
[116] Ibid., p. 10 and 12.
[117] Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 103).
[118] OECD, Consumer vulnerability in the digital age, 2023, p. 43.
[119] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ 2017, L 345, p. 1).
[120] Article 68 GDPR.

court has always been accompanied with high accessibility thresholds for individuals. Whilst collective redress is more common in the consumer protection field, it is still an emerging phenomenon in the data protection field.[121] In that regard, the recent judgement of the CJEU that confirmed that consumer protection associations may bring representative actions against infringements of personal data protection is promising.[122] The finding that certain commercial practices might at the same time be qualified as an infringement of the GDPR and the UCPD gives data subjects/consumers, and the organisations that represent them, a larger choice of remedies and ways to hold data controllers/traders to account.

V. CONCLUSION

The personalisation of in-game commercial practices in videogames occurs at the crossroads of the consumer and data protection framework at the level of the EU. Through an analysis of three concepts present in both frameworks – fairness, transparency and vulnerability – this paper addresses the interplay of both sets of rules to ensure adequate protection of players, especially children. In brief, videogame companies – when operating as both trader and data controller – must consider the limits imposed by the data and consumer protection frameworks on the personalisation of in-game content for commercial purposes. Although it is not unimaginable that videogames also personalise the gameplay experience or in-game offers to the benefit of the player, personalisation practices might also be unfair, untransparent and manipulative, breaching one or both frameworks. Especially for children, the consensus is increasingly developing towards a general prohibition on profiling for commercial purposes, which includes personalisation practices in videogames based on constructed user profiles. The higher threshold of protection for children originates from their increased susceptibility or vulnerability to manipulative practices. Although such a prohibition is not included explicitly in the GDPR (although it has been hinted at by the WP29), nor the UCPD, in the future, perhaps additional practices could be included on the blacklist provided in the UCPD, especially those practices where personalised content is offered based on profiles created by using behavioural data of children to increase engagement with the videogame.

However, the importance of protecting adult consumers should not be overlooked, as they may be equally or 'universally' vulnerable when engaging with personalised videogame offers for commercial purposes. In an era where videogame monetisation is increasingly integrated into the gameplay experience and increasingly relies on analysis of big data sets of players, a combination of data protection and consumer protection may be necessary to ensure adequate protection for all players against practices that breach their autonomy.

[121] Article 80 GDPR.
[122] CJ, Judgment of 28 April 2022, *Meta Platforms Ireland,* C-319/20, ECLI:EU:C:2022:322.

REFERENCES

INTERNATIONAL LAW

United Nations Committee for the Rights of the Child, General Comment 25 on children's rights in relation to the digital environment, 2021.

EUROPEAN UNION LAW

1. Primary law

Treaty on the European Union (OJ 2012, C 326, p. 13).

Treaty on the Functioning of the European Union (OJ 2012, C 326, p. 47).

Charter of Fundamental Rights of the European Union (OJ 2012, C 326, p. 391).

2. Secondary law

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, amended by Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019, (OJ 1993, L 95, p. 29).

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

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

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

Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ 2017, L 345, p. 1).

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 (OJ 2019, L 136, p. 1).

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 (OJ 2022, L 277, p. 1).

3. Other policy documents

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 2017.

Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', 2017.

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 2018, <https://edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf>.

European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0), 2020.

Communication COM/2020/696 from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0696>.

European Data Protection Board, Guidelines 8/2020 on the targeting of social media users, 2021.

Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 1).

Commission Notice C/2021/9314 Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (OJ 2021, C 525/01, p. 1).

Commission Notice C/2021/9320 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (OJ 2021, C 526, p. 1).

European Data Protection Board, Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 2022.

European Parliament, Resolution of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI)), 2023.

4. Case law

AG Trstenjak, Opinion of 29 November 2011, *Perenicova and Perenic,* C-453/10, ECLI:EU:C:2011:788, para. 90.

CJ, Judgment of 5 December 2013, *Vapenik,* C-508/12, ECLI:EU:C:2013:790.

CJ, Judgment of 2 May 2019, *Pillar Securitisation*, C-694/17, ECLI:EU:C:2019:345.

CJ, Judgment of 28 April 2022, *Meta Platforms Ireland,* C-319/20, ECLI:EU:C:2022:322.

European Data Protection Board, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR).

LITERATURE

A. Drachen et al., "Game Data Mining" in M. El-Nasr, A. Drachen and A. Canossa (eds*) "Game Analytics: Maximizing the Value of Player Data"*, Springer, 2013.

A. Drachen, M. El-Nasr and A. Canossa, "Game Analytics - The Basics" in M. El-Nasr, A. Drachen and A. Canossa (eds), *Game Analytics: Maximizing the Value of Player Data,* Springer, 2013.

B. Keirsbilck, "Interaction between Consumer Protection Rules on Unfair Contract Terms and Unfair Commercial Practices", 2013, *50 Common Market Law Review 247*.

C.B. Hart, "The Evolution and Social Impact of Video Game Economics", Lexington Books, 2020.

C. Riefa, "Protecting Vulnerable Consumers in the Digital Single Market", *33 European Business Law Review 612*, 2022.

C. Willet, "Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive", *33 Journal of Consumer Policy 247,* 2010.

D. King, P. Delfabbro, S. Gainsbury, M. Dreier, N. Greer and J. Billieux, "Unfair play? Video games as exploitative monetized services: An examination of game patents from a consumer protection perspective", *101 Computers in Human Behavior 131*, 2019.

D. Zendle, R. Meyer and N. Ballou, "The changing face of desktop videogame monetization: An exploration of exposure to loot boxes, pay to win, and cosmetic microtransactions in the most-played *Steam* games of 2010-2019", *15(5) PLoS ONE,* 2020.

D. Zendle, R. Meyer, P. Cairns, S. Waters and N. Ballou, "The prevalence of loot boxes in mobile and desktop games" *115(9) Addiction,* 2020.

E. Gibson, M. Griffiths, F. Calado and A. Harris, "Videogame player experiences with micro-transactions: An interpretative phenomenological analysis" *145 Computers in Human Behavior 107766,* 2023.

G. Sartor and F. Lagioia, "The impact of the General Data Protection Regulation (GPDR) on artificial intelligence" (Study commissioned by the European Parliamentary Research Services), 2020, p. 59, retrieved from <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>.

J. Reynolds, "Gambling on Big Data: Designing Risk in Social Casino Games", *10(1) European Journal of Risk Regulation 116*, 2019.

J. Svelch, "Normalizing player surveillance through video game infographics", *New Media & Society 1*, 2022.

J. Zhu and S. Ontañón, "Player-Centered AI for Automatic Game Personalization: Open Problems", *arXiv 2102:07548*, 2021.

K. Alha, "The Rise of Free-to-Play: How the revenue model changed games and playing", Tampere University, 2020.

K. Purnhagen, "More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?" *8(2) European Journal of Risk Regulation 437*, 2017.

K. Sigmon, "Pay to Play: Video Game Monetization Patents and the Doctrine of Moral Utility", *5 Georgetown Law Technology Review 72*, 2021.

L. Van Roessel and J. Svelch, "Who Creates Microtransactions: The Production Context of Video Game Monetization", in O. Sotamaa and J. Svelch (eds) *Game Production Studies,* Amsterdam University Press, 2021.

M. Bonenfant, A. Dumon and L. St-Martin, "Being played in everyday life: Massive data collection on mobile games as part of ludocapitalist surveillance dispositive" in L. Samuelsson, C. Cocq, S. Gelfgren and J. Enbom (eds), *Everyday life in the culture of surveillance",* Nordicom, 2023.

M. Davidovici-Nora, "Innovation in business models in the videogame industry: Free-To-Play or the gaming experience as a service" *2(3) The Computer Games Journal 22,* 2013.

N. Helberger, F. Borgesius and A. Reyna, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *54(5) Common Market Law Review*, 2017.

N. Helberger, M. Sax, J. Strycharz and H. Micklitz, "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability", *45 Journal of Consumer Policy 175*, 2022.

P. Cartwright, "Understanding and protecting vulnerable financial consumers" *38 Journal of Consumer Policy 119*, 2014.

P. Hacker, "Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law", *European Law Journal*, 2021.

S. Karpinskyj, F. Zambetta and L. Cavedon, “Video game personalisation techniques: A comprehensive survey”, *5 Entertainment Computing 211*, 2014.

T. Crepax and J. T. Muehlberg, “Upgrading the Protection of Children from Manipulative and Addictive Strategies in Online Games: Legal and Technical Solutions beyond Privacy Regulation”, *31 The International Review of Information Ethics*, 2022.

V. Verdoodt, “Children’s Rights and Commercial Communication in the Digital Era. Vol. 10.”, Intersentia, 2022.

V. Verdoodt, E. Lievens, E and A. Chatzinikolaou, “The EU Approach to Safeguard Children’s Rights on Video-Sharing Platforms: Jigsaw or Maze?”, *Media and Communication, 11(4)*, 2023.

REFERENCES TO WEBSITES

BEUC, “Automated decision making and Artificial Intelligence - A consumer perspective BEUC Position Paper”, 2018, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf>.

BEUC, “The Manipulated Consumer, The Vulnerable Citizen - BEUC’s response to European Democracy Action Plan”, 2020, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-075_the_manipulated_consumer_the_vulnerable_citizen.pdf>.

BEUC, EU Consumer Protection 2.0 Structural asymmetries in digital consumer markets, 2021, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf>.

BEUC, “Dark Patterns” and the EU Consumer Law Acquis: Recommendations for better enforcement and reform, 2023, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf>.

BEUC, “Towards European Digital Fairness - BEUC Framing Response Paper For The Refit Consultation”, 2023, <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf>.

Data Protection Commission (Ireland), “Fundamentals for a Child-Oriented Approach To Data Processing”, 2018, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>.

E. Petrovskaya, S. Deterding and D. Zendle, “Prevalence and Salience of Problematic Microtransactions in Top-Grossing Mobile and PC Games: A Content Analysis of User Reviews” *CHI Conference on Human Factors in Computing Systems,* 2022, retrieved from <https://doi.org/10.1145/3491102.3502056>.

European Commission, “Digital fairness – fitness check on EU consumer law”, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en>.

European Commission, Consumer vulnerability across key markets in the European Union, 2016, <https://op.europa.eu/en/publication-detail/-/publication/d1af2b47-9a83-11e6-9bca-01aa75ed71a1/language-en>.

European Parliament, Briefing on Vulnerable Consumers, 2021, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI(2021)690619_EN.pdf>.

G. Couneson et al., “Gaming Series #2: Online Safety and Gaming – EU and UK Approaches to Regulation”, Linklaters Tech Insights, 2023, <https://techinsights.linklaters.com/post/102ig9a/gaming-series-2-online-safety-and-gaming-eu-and-uk-approaches-to-regulation>.

J. Clement, “Global Video Game Users 2027”, 2023, <https://www.statista.com/statistics/748044/number-video-gamers-world/>.

Newzoo, “Global Games Market Report 2023”, 2023, <https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2023-free-version>.

OECD, Consumer vulnerability in the digital age, 2023, <https://www.oecd-ilibrary.org/docserver/4d013cc5-en.pdf?expires=1698309562&id=id&accname=guest&checksum=B0C01C719E98DEBE147D7398F6022E65>.

P. Rott, J. Strycharz, F. Alleweldt, “Personalised Pricing”, a Study requested by the IMCO Committee of the European Parliament, 2022, <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/734008/IPOL_STU(2022)734008_EN.pdf>.

S. Mukherjee, K. Pothong, K and S. Livingstone (Digital Futures Commission, 5Rights Foundation), “Child Rights Impact Assessment: A tool to realise child rights in the digital environment”, 2023, <https://digitalfuturescommission.org.uk/wp-content/uploads/2022/06/Child-Rights-Impact-Assessment.pdf>.

S. Read, “Gaming Is Booming and Is Expected to Keep Growing. This Chart Tells You All You Need to Know.”, 2022, <https://www.weforum.org/agenda/2022/07/gaming-pandemic-lockdowns-pwc-growth/>.

Statista Market Insights, “Games – Worldwide”, 2022, <https://www.statista.com/outlook/dmo/app/games/worldwide>.

The Business Research Company, “Online Microtransaction Global Market Report”, 2023, <https://www.thebusinessresearchcompany.com/report/online-microtransaction-global-market-report>.

Videogames Europe and European Games Developers Federation, “All about videogames – European Key Facts 2022”, 2022, <https://www.videogameseurope.eu/wp-content/uploads/2023/08/Video-Games-Europe_Key-Facts-2022_FINAL.pdf>.