How the AI Act Applies to E-Commerce

by **Elif Cansu Yaşar ***

Abstract: This article researches the following questions: To what extent do the provisions of the AI Act apply to e-commerce companies that use AI? To what extent is this in line with the objectives of the AI Act, considering the risks in relation to the use of AI for e-commerce?

The AI Act has a risk-based approach. For e-commerce companies to comply with the AI Act, it is important to know how applicable it is to their activities. Some e-commerce activities might be under the prohibited practices in the AI Act. However, most of the e-commerce activities are not entirely regulated by it since they are not classified as high-risk AI systems under the AI Act. Since e-commerce can pose serious risks, especially regarding manipulation and discrimination, the AI Act leaves a regulatory gap in the use of AI in e-commerce.

Keywords: AI; AI Act; E-Commerce

Recommended citation: Elif Cansu Yaşar, How the AI Act Applies to E-Commerce, 15 (2024) JIPITEC 38 para 1.

A. Introduction

1 E-commerce made its appearance almost simultaneously with the rise of the internet. Because of the risks and challenges brought by economic growth and advancing technologies, it soon attracted regulatory attention. E-commerce has been regulated in various aspects under the EU law since A European Initiative in Electronic Commerce in 1997[1].

2 In recent years, online shopping has gained popularity, with the rise of online platforms and more recently, with the Covid-19 pandemic. Europe E-commerce's 2022 report states that "in 2021, total European e-commerce grew to €718bn with a growth rate of 13%"[2] and the changes in the sector, such as digitalisation, require businesses to invest more in the future to keep up with them.[3] With this digitalisation trend, the use of AI in e-commerce activities such as big data analytics, data management, customer insights, personalisation, marketing, custom-made advertisements and targeting has also increased.[4]

3 Currently, in addition to the Directive on Electronic

* PhD Candidate, Radboud Business Law Institute (OO&R), Radboud University, Nijmegen (The Netherlands). cansu.yasar@ru.nl

1 Commission, 'A European Initiative in Electronic Commerce', (Communication) COM (97) 157 final

2 Ecommerce Europe, EuroCommerce for retail & wholesale, 'European E-Commerce Report' (2022) <https://ecommerce-europe.eu/wp-content/uploads/2022/06/CMI2022_FullVersion_LIGHT_v2.pdf> accessed 12 October 2023, 2

3 Ecommerce Europe (n 2), 3

4 Ecommerce Europe (n 2), 2, 3, 20 24, 28, 34, 38, 48, 55, 58, 82

Commerce,[5] there are EU rules regulating various aspects of e-commerce activities. This includes rules in the areas of product safety and liability, fundamental rights[6] and consumer rights.[7] In principle, these rules are fully applicable regardless of the involvement of AI.[8] For example, if personal data is processed through the use of AI, the GDPR applies. Most notably, Article 22 of the GDPR specifically regulates "automated individual decision-making, including profiling".[9]

4 The Shaping Europe's Digital Future program aims to ensure that EU rules are technologically, economically, and socially compatible with the digital age.[10] This includes the Digital Services Act[11] and the Digital Markets Act.[12] Another important regulation is the Regulation laying down harmonised rules on artificial intelligence (AI Act).[13] The AI Act adopts a risk-based approach and prohibits, regulates, or leaves unregulated certain AI practices depending on their classification into risk categories. From the e-commerce perspective, some of the rules in the AI Act such as those on the prohibited practices may overlap to some extent with other legislation. However, The AI Act differs from the previous instruments since it introduces transparency rules for certain AI systems.

5 It is important for practitioners and legal scholars to examine the AI Act from the e-commerce perspective. E-commerce companies which increasingly use AI in their activities must know to what extent this new regulation applies to them. In order to understand their obligations, they must know which risk category they belong to, their roles under the AI Act, and which of their activities require more legal attention. For legal scholars and legal practitioners, it is important to know the AI techniques used in e-commerce, purposes and reasons for using different techniques so that they can evaluate the legal implications of these techniques and see to what extent the AI Act addresses them.

5 Directive 2000/31/EC of the European Parliament And of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

6 Such as 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) [2016] OJ L 119, 04.05.2016 (GDPR) in data protection and privacy

7 Such as 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 L 149, 11.6.2005, p. 22–39) (Unfair Commercial Practices Directive) and 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 OJ L 304, 22.11.2011, p. 64–88 (Consumer Rights Directive)

8 European Commission, 'White Paper on Artificial Intelligence - A European approach to excellence and trust' COM (2020) 65 final, 13

9 About AI and the application of the GDPR, see also: Sebastião Barros Vale, 'GDPR and the AI Act Interplay: Lessons from FPF's ADM Case-Law Report' (Future of Privacy Forum, 3 November 2022) <https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/> accessed 12 October 2023

10 Commission, 'Shaping Europe's Digital Future' (19 February 2020) <https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future-feb2020_en.pdf> accessed 6 March 2024

11 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, 27.10.2022

12 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265, 12.10.2022 (Digital Markets Act)

13 European Parliament, 'European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))' (Texts Adopted) P9_TA(2024)0138

6 The risks that may arise from the use of AI in e-commerce have previously been examined from data protection and privacy law,[14] consumer law,[15] and discrimination law[16] perspectives. However, although there has been literature about how the AI Act regulates issues such as manipulation,[17] discrimination,[18] and data protection,[19] current literature has not dealt with the question of whether the AI Act applies to e-commerce companies and what does the AI Act mean for e-commerce. Examining the use of AI in e-commerce from an AI Act perspective therefore complements earlier work in the literature.

7 This article researches the following questions: *To what extent do the provisions of the AI Act apply to e-commerce companies that use AI? To what extent is this in line with the objectives of the AI Act, considering the risks in relation to the use of AI for e-commerce?* To answer this question, this article will first determine the extent to which the AI Act applies to the use of AI in e-commerce activities. Then, it will assess whether the risks of using AI in e-commerce should be regulated under the AI Act or whether the protection against these risks in existing EU legislation is sufficient. This article finds out that some activities of e-commerce companies might be prohibited under the AI Act. However, the prohibited practices under the AI Act require many conditions that will not always be met. E-commerce activities do not fall into the high-risk classification under the AI Act, which includes a large part of the obligations. However, the transparency obligations for certain AI systems apply to e-commerce activities.

8 Within the scope of the article, "e-commerce" refers to the activities of companies that sell their own products on their websites and on platforms. The online platforms that facilitate these e-commerce companies are outside of the definition. This article is limited to B2C e-commerce activities of companies that sell physical goods online. However, the analysis may also be relevant for services. The AI Act may intersect with other legislation. Such as the GDPR, especially in the provisions related to data quality.

14 European Parliament, Directorate-General for Parliamentary Research Services, Giovanni Sartor, Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' Panel for the Future of Science and Technology PE 641.530 – June 2020; Jozef Andraško, Matúš Mesarčík, Ondrej Hamuľák, 'The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework' (2021) 36 AI & Society 623

15 Marco Lippi and others, 'The Force Awakens: Artificial Intelligence for Consumer Law' (2020) 67 Journal of Artificial Intelligence Research 169; Agnieszka Jabłonowska and others, 'Consumer law and artificial intelligence: challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence : final report of the ARTSY project' (2018) EUI Department of Law Research Paper No. 2018/11 <https://ssrn.com/abstract=322805> accessed 16 March 2024

16 Frederik Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe, Directorate General of Democracy, 2018); Frederik Zuiderveen Borgesius, Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) Journal of Consumer Policy

17 Huixin Zhong, Eamonn O'Neill, Janina A. Hoffmann, 'Regulating AI: Applying insights from behavioural economics and psychology to the application of article 5 of the EU AI Act' (The 38th Annual AAAI Conference on Artificial Intelligence, Canada, 20 February 2024 - 27 February 2024 <https://arxiv.org/pdf/2308.02041.pdf > accessed 16 March 2024; Matija Franklin and others, 'Missing Mechanisms of Manupilation in the EU AI Act' (The International FLAIRS Conference Proceedings 35, 4 May 2022) <https://journals.flvc.org/FLAIRS/article/view/130723> accessed 16 March 2024; Risto Uuk, 'Manipulation and the AI Act' (Future of Life Institute, 18 January 2022) <https://futureoflife.org/wp-content/uploads/2022/01/FLI-Manipulation_AI_Act.pdf > accessed 16 March 2024

18 Marvin van Bekkum, Frederik Zuiderveen Borgesius, 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?' (2023) 48 Computer Law & Security Review 105770; Salih Tayfun İnce, 'European Union Law and Mitigation of Artificial Intelligence-Related Discrimination Risks in the Private Sector: With Special Focus on the Proposed Artificial Intelligence Act' (2021) 71 Annales de la Faculté de Droit d'Istanbul 71

19 Barros Vale (n 9); Raphaël Gellert, 'The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?' (2021) 3 Journal of Ethics and Legal Technologies 15; Joanna Mazur, 'Artificial Intelligence vs Data Protection: How the GDPR Can Help to Develop a Precautionary Regulatory Approach to AI?' in Angelos Kornilakis and others (eds), *Artificial Intelligence and Normative Challenges: International and Comparative Legal Perspectives* (Springer, Cham 2023)

Although the AI Act may include provisions on the use of (both personal and non-personal) data, it focuses more on the safety of AI systems. Data protection issues are regulated by the GDPR. Therefore, in line with the focus on the AI Act, this article will focus on the risks and safety issues when using AI, rather than the data protection issues. The AI Act may also intersect with the Unfair Commercial Practices Directive regarding the prohibited practices and might introduce complementary rules to issues that are already regulated in consumer law. However, as this article seeks to find out whether the AI Act is applicable to e-commerce, an analysis of consumer law falls outside of its scope.

9 Section B explores how AI can be used in e-commerce activities. Section C examines the risks arising from these activities. Section D analyses the AI Act and its risk-based approach in relation to the risks of e-commerce activities. Since the AI Act brings different requirements for different risk levels, applicability will be analysed separately for each risk level.

10 After the European Commission's Proposal in 2021,[20] the Council of the European Union published its General Approach on 6 December 2022, and the European Parliament adopted its Negotiating Position on 14 June 2023. They have reached a provisional agreement on 9 December 2023. The Compromise Text was published on 26 January 2024.[21] On 13 March 2024, the European Parliament adopted the AI Act and in May 2024, it was approved by the Council. Unless stated otherwise, this article refers to the Adopted Text by the European Parliament.[22]

B. AI Use in E-Commerce

11 Artificial Intelligence is a technology that is difficult to capture in a precise definition. However, it can be explained in terms of its function. It could be defined as "technologies programmed to analyse the world around them and take action to achieve specific goals",[23] or as "a collection of technologies that combine data, algorithms and computing power".[24]

12 AI systems can be used in e-commerce in many ways. The uses can be broadly divided into the analysis of data, making business decisions according to the inferences from the collected data, and using AI during the sales or after sales. Since these systems often interact with each other, it is not possible to clearly distinguish the phases. Personalisation, for instance, can be used in many stages of e-commerce activities such as marketing, sales, and after-sales. However, considering the business steps of an e-commerce company, the use of AI can be examined as follows.

I. Customer Insights, Predictions, and Pricing

13 Firstly, businesses can use AI to gain more insight on existing or potential customers. Analysing customer behaviour (such as purchasing behaviour) is crucial for e-commerce businesses. It allows them to shape their services accordingly.[25] AI may answer questions such as: do customers compare prices before buying or how likely are they to make a purchase? Customer behaviour analysis can be used to identify online browsing and purchase behaviours of customers.[26] Companies can learn what kind of products customers search for, how much time they spend on these pages, their buying patterns,

20 Commission, 'Proposal for A Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM/2021/206 final (AI Act).

21 Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement' (Note) 5662/24

22 European Parliament, 'European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))' (Texts Adopted) P9_TA(2024)0138

23 European Commission, 'Artificial Intelligence' (Shaping Europe's digital future, last update 31 august 2022) <https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence> accessed 12 October 2023

24 COM (2020) 65 final, 2

25 Lucas Micol Policarpo and others, 'Machine learning through the lens of e-commerce initiatives: An up-to-date systematic literature review' (2021) 41 Computer Science Review 100414, 2

26 Countants, 'Why Consumer Behavior Analysis Is So Relevant to the eCommerce business?' (Medium, 6 January 2020) <https://medium.datadriveninvestor.com/why-consumer-behavior-analysis-is-so-relevant-to-the-ecommerce-business-8f49c250ca9c> accessed 12 October 2023

and how they react to personalisation or discounts.[27] Customer behaviour on websites and mobile apps can be analysed for this,[28] as well as email behaviour such as whether emails have been read or redirected customers to the website.[29]

14 Companies can make use of customer segmentation to group customers according to various attributions such as age, location, gender, and shopping patterns,[30] and offer personalised services to different groups. Companies can use predictive analytics to understand the past behaviours of customers and make predictions about their preferences in the future.[31] Data such as "past click through behaviour, shopping history, browsing patterns, product preferences" can be analysed to answer questions such as how much money customers are likely to pay for a product or to make personalised recommendations.[32] Churn prediction can be used to retain customers by noticing if customers stop their regular purchases and offering personalised discounts to them.

15 AI can also be used in pricing strategies. Dynamic pricing can be beneficial to increase sales since it allows businesses to determine competitive prices and reach more customers.[33] AI systems can take different factors into account when using dynamic pricing. They can use data about the company rather than the customer, such as supply and demand or the fees of other companies.[34] They can also use data about customers such as age, location, devices they use or their shopping habits.[35] Personalised offers and personalised pricing can help to increase sales by making the customer feel more recognised by the company.[36]

II. Marketing

16 Once companies analyse the data and know more about their customers, they can benefit from using AI in promoting their products to their customers. Firstly, AI can determine the most suitable time for an advertisement, or the most effective channel, such as email, social media, or phone notifications.[37] Email communications with customers can be personalised and can be used for various purposes. It is possible to send a reminder email for an abandoned cart, for personalised offers or announcements.[38]

17 Recommender systems can be widely used for marketing. It is often possible to implement them according to the different needs and purposes of companies. Depending on the implemented technique, data such as user feedback, user ratings, number of purchases, item price, purchase history, browsing history or product characteristics can be used for making recommendations.[39] Personalisation can increase sales by offering personalised recommendations to customers who are not sure what they are searching for, or who find it difficult to make a decision because of the number of products

27 *Ibid*

28 Countants, 'How Artificial Intelligence is transforming the E-commerce Industry' (Medium, 10 May 2019) <https://medium.com/@Countants/how-artificial-intelligence-is-transforming-the-e-commerce-industry-countants-scalable-custom-73ae06836d35> accessed 12 October 2023

29 Countants, 'Why Consumer Behavior Analysis Is So Relevant to the eCommerce business?' (n 26)

30 ProjectPro, '10 Machine Learning Projects in Retail You Must Practice' (ProjectPro, last updated 12 October 2023) <https://www.projectpro.io/article/machine-learning-projects-in-retail-and-ecommerce/498> accessed 12 October 2023

31 IQLECT, 'The Importance of Predictive Analytics for E-commerce Stores' (Medium, 14 November 2018) <https://medium.com/swlh/the-importance-of-predictive-analytics-for-e-commerce-stores-d7ef0ce2d32e> accessed 12 October 2023

32 *Ibid*

33 Cem Dilmegani, 'Ecommerce Dynamic Pricing in 2023: Guide & Examples' (AI Multiple, Published 25 October 2021, Updated 12 October 2023) <https://research.aimultiple.com/dynamic-pricing-ecommerce/> accessed 12 October 2023

34 Cem Dilmegani, 'Ultimate Guide to Dynamic Pricing in 2023: Roadmap & Vendors' (AI Multiple, Updated 4 August 2023) <https://research.aimultiple.com/dynamic-pricing/> accessed 12 October 2023

35 *Ibid*

36 'Ecommerce Personalization: How to Make Each Customer Feel Like a VIP' (Big Commerce) <https://www.bigcommerce.com/articles/ecommerce/personalization/> accessed 12 October 2023

37 'How to leverage AI in marketing: three ways to improve consumer experience' (Deloitte) <https://www2.deloitte.com/si/en/pages/strategy-operations/articles/AI-in-marketing.html> accessed 12 October 2023

38 Brittany Shulman, 'How to launch a successful personalized marketing strategy' (Bazaarvoice, 4 January 2022) <https://www.bazaarvoice.com/blog/how-to-launch-a-successful-personalized-marketing-strategy/#h-what-is-personalized-marketing> accessed 12 October 2023

39 *Ibid*, 81-82 Table 1

to choose from.[40] Customer loyalty programs with personalised rewards can increase the loyalty of customers to the seller.[41]

III. Sales and After-Sales

18 AI can be used in sales and after-sales to provide convenience to the customers and the company.

19 Search-related AI applications help customers find what they are looking for more easily and therefore, increase sales. Using autocomplete in search buttons can help customers find what they are looking for, suggest the products they missed, or show them relevant results in case they misspell the product name.[42] Search results can be personalised, or recommendations for certain groups or locations can be used.

20 Voice search allows customers to find what they are looking for more easily, without having to type anything.[43] With visual search, customers can take a photo and search for similar products. Product tags can be used in images so that the customers can purchase the different products in one image.[44] With Augmented Reality, customers can virtually try on products such as clothes and cosmetics, and they can see how furniture or home decoration will look in their homes before purchasing them.[45]

21 Chatbots can answer product-related questions, act as an always-available customer service tool, or make product recommendations.[46] This reduces the company's workload and increases the customer satisfaction by enabling them to reach the company at any time.

22 Sentiment analysis can be used to better understand purchasing decisions or the overall opinion of customers. By analysing the product reviews on the e-commerce website or social media with Natural Language Processing (NLP) techniques, companies can have an insight into the customers' view of the company and the product and make future business plans accordingly.[47] NLP can also be used for intelligent search, which helps customers to find the products they are searching for by making accurate predictions.[48] These techniques can be used together with personalisation and recommendations, and therefore be very effective for the business.[49]

C. Risks of Using AI In E-Commerce

23 AI systems entail various risks for both customers and companies.[50] On one hand, algorithmic decision-making can leave customers vulnerable, and customers might worry that AI will have unforeseen effects and that it can be used with malicious intent. Although there are regulations protecting the fundamental rights of individuals, the use of AI can make their implementation more difficult due to some specific features of it.[51] On the other hand, companies might worry about the (uncertain)

40 'Ecommerce Personalization: How to Make Each Customer Feel Like a VIP' (Big Commerce) <https://www.bigcommerce.com/articles/ecommerce/personalization/> accessed 12 October 2023

41 *Ibid*

42 Jon Silvers, '15 Best Practices for 2022 to Improve E-commerce Site Search' (Algolia, 31 July 2023) <https://www.algolia.com/blog/ecommerce/15-best-practices-for-ecommerce-on-site-search/> accessed 12 October 2023

43 Nick Brown, 'How to Optimize Voice Search Feature for Your Ecommerce Store' (Big Commerce) <https://www.bigcommerce.com/blog/voice-search-ecommerce/> accessed 12 October 2023

44 'How Visual Search has transformed the modern shopping experience', (Visenze, 21 March 2019) <https://www.visenze.com/blog/2019/03/21/how-visual-search-has-transformed-the-modern-shopping-experience/> accessed 12 October 2023

45 Helen Papagiannis, 'How AR Is Redefining Retail in the Pandemic' (Harvard Business Review, 7 October 2020) <https://hbr.org/2020/10/how-ar-is-redefining-retail-in-the-pandemic> accessed 12 October 2023

46 Cem Dilmegani, 'Sales Chatbots in 2023: Top Use Cases & Best Practices' (AI Multiple, Updated 9 October 2023) <https://research.aimultiple.com/sales-chatbot/> accessed 12 October 2023

47 Begüm Yılmaz, 'E-Commerce Sentiment Analysis in 2023: Top 3 Applications' (AI Multiple, Updated 8 September 2023) <https://research.aimultiple.com/ecommerce-sentiment-analysis/> accessed 12 October 2023

48 'The Future of Shopping: Natural Language Processing Applications in E-Commerce' (Defined AI, 29 July 2020) <https://www.defined.ai/blog/the-future-of-shopping-natural-language-processing-applications-in-e-commerce/> accessed 12 October 2023

49 *Ibid*

50 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) para 2

51 COM (2020) 65 final, 10

implications of relevant legal provisions when AI is used.[52] However, the AI Act focuses on the risks of AI systems for natural persons. Therefore, this article will focus only on these risks.

24 Since the AI Act has a risk-based approach, its obligations depend on the risks of an AI system. This section will examine the risks of AI use in e-commerce independently from the provisions of the AI Act. The most important risks for customers brought by the use of AI in e-commerce can be divided into two main groups. These are manipulation and discrimination risks.

I. Manipulation

25 Manipulation can be used to sell certain products, sell more products or trigger impulse buying. Companies often use manipulation in marketing to influence customers' decision-making by deceiving them or "playing on a vulnerability".[53] Not every technique that drives customers to buy a particular product is manipulative. These can also be persuasion methods based on accurate information.[54] However, especially with the developing technology, it became easier to manipulate customers through methods such as deliberately hiding some information or presenting it to customers at a certain time.[55]

26 Manipulation can be in extreme forms, such as dark patterns. Dark patterns are design choices intended to deceive people with false suggestions such as that various prices will only stay this way for a certain period or that there is less product in stock than there actually is.[56] In addition to the AI Act, various EU legislation such as the Unfair Commercial Practices Directive and the GDPR include rules that may apply to certain aspects of dark patterns. For example, the Unfair Commercial Practices Directive protects customers against practices that "impair consumer's ability to make an informed decision".[57] In cases where personal data is involved, the GDPR may provide protection against dark patterns with rules such as the fairness principle[58] and privacy by design and default obligation.[59] However, the European Parliament found that the existing legislation on addictive design choices such as dark patterns did not provide sufficient protection to consumers and called on the Commission to close the regulatory gaps regarding the "addictive design of online services".[60]

27 Manipulation can be used for targeting vulnerable groups and exploiting their vulnerability. It also has negative effects on the average customer. Manipulation can have economic or psychological consequences. It can cause economic damage to customers by making them buy products that they did not actually want to buy.[61] Moreover, it can harm "autonomy" by affecting people's right to make their own decisions about themselves.[62]

28 AI and especially personalisation can be used by e-commerce companies to trigger impulse buying. Impulsive buying refers to the inability to resist buying.[63] Impulsive buying can be stimulated by personalisation. Even though personalisation can be very beneficial for both customers and companies, over-personalisation also has downsides. It can be used to make customers spend more money rather than benefit them.[64] If customers, especially

52 *Ibid*, 9

53 Shlomo Sher, 'A Framework for Assessing Immorally Manipulative Marketing Tactics' (2011) 102 Journal of Business Ethics 97, 99, 100

54 Gilles N'Goala, 'Opportunism, transparency, manipulation, deception and exploitation of customers' vulnerabilities' in Bang Nguyen, Lyndon Simkin, Ana Isabel Canhoto (eds) *The Dark Side of CRM Customers, Relationships and Management* (Routledge 2015)

55 Tal Zarsky, 'Privacy and Manipulation in the Digital Age' (2019) 20(1) Theoretical Inquires in Law 157, 158

56 Ray Sin and others, 'Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying?" (2022) Behavioural Public Policy 1, 3

57 Unfair Commercial Practices Directive art 2(e), 5(2)

58 GDPR art 5(1)(a)

59 GDPR art 25; For an evaluation of various EU legislation regarding dark patterns see: Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' TILEC Discussion Paper No. 2023-07, (Tilburg Law School Research Paper)

60 European Parliament, 'Addictive design of online services and consumer protection in the EU single market European Parliament resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI))' (Texts Adopted) P9_TA(2023)0459

61 Zarsky, 'Privacy and Manipulation in the Digital Age' (n 55) 172, 173

62 *Ibid*, 173, 174

63 Dennis W. Rook, 'The Buying Impulse' (1987) 14 The Journal of Consumer Research 189, 191

64 Aniko Hannak and others, 'Measuring Price Discrimination

from vulnerable groups cannot adequately protect themselves from these techniques designed to make them spend more, this can lead to overspending and negative economic effects.

II. Discrimination

29 Another important problem that can arise with the use of AI is discrimination. In e-commerce, discrimination may lead to price discrimination, limited or no access to goods/services, or differences in the quality of the products. People might be subjected to discrimination as a result of the inferences made from their shopping habits or age, gender, or zip code.

30 Especially the opacity of some AI systems can make it difficult to determine whether discrimination exists and, if so, on what basis.[65] Discrimination can be direct or indirect. Direct discrimination is the discrimination of people over a "protected characteristic" such as gender or race.[66] Indirect discrimination is when an application that appears neutral at first discriminates over any protected characteristic.[67] In e-commerce, it is more likely to encounter indirect discrimination than direct discrimination. For example, it is possible that more people from a certain racial group live in a particular zip code area.[68] Different results that people may see on websites are more likely to be due to the zip code, rather than racial origin.

31 Discrimination can be intentional or unintentional. If organisations have the intention to discriminate, they can choose factors such as "target variable" and "class label" that will affect the AI's decision-making according to their intentions.[69] The target variable means to express the result that the organisation wants to reach in a technical way that the algorithms can understand.[70] Class labels are labelling of the data used to reach these results.[71] For example, in e-commerce, the target variable could be finding the type of customer most likely to buy a product. To reach this result, different variables can be considered such as the number of purchases the customers have made, the products they have purchased, or the amount of money they have spent. Companies can choose which of these variables to consider. However, the choices made in this target variable and class labels can also cause unintentional indirect discrimination.[72] In addition, if the training data used in an AI system are biased, the AI system might reflect this bias.[73]

32 E-commerce companies can constantly change their prices and show different prices to certain groups or even individuals. This is because a company would like to charge the highest price customers are willing to pay for a particular product.[74] The more data companies have about customers, the easier it gets to determine the highest price customers will pay for a product.[75] However, seeing different prices on websites cannot always be attributed to personalisation, and there might be different reasons such as the stock status, updates to the website or technical reasons.[76] A study on this subject found that only one of the ten retail websites they examined showed different prices to iOS and Android users, and the price difference was very low in practice.[77] Due to the opacity of AI, it is difficult to determine whether the different prices seen on e-commerce sites are based on personalisation. There may also be commercial or technical reasons for these different prices.

33 Since companies use personal data such as IP

and Steering on E-commerce Web Sites' (2014) IMC '14: Proceedings of the 2014 Conference on Internet Measurement Conference 305, 305

65 Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (n 16), 10

66 *Ibid*, 18

67 *Ibid*, 19

68 *Ibid*, 13

69 *Ibid*, 10,11; Solon Barocas, Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671, 678, 692

70 Barocas, Selbst (n 69), 678

71 *Ibid*, 678

72 Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (n 16), 11

73 *Ibid*, 10, 12

74 Marc Bourreau, Alexandre de Streel, Inge Graef, 'Big Data and Competition Policy: Market power, personalised pricing and advertising' (Project Report, Centre on Regulation in Europe, 2017), 39

75 *Ibid*, 40

76 Aniko Hannak and others, 'Measuring Price Discrimination and Steering on E-commerce Web Sites' (2014) IMC '14: Proceedings of the 2014 Conference on Internet Measurement Conference 305, 307

77 *Ibid*, 315,316

addresses and cookies to identify customers, these practices mostly fall within the scope of data protection rules.[78] However, price discrimination also has economic effects. It can have a positive economic impact on companies as it allows them to charge more for the same product than people who are willing to pay more. On the other hand, considering the "distribution of welfare" between companies and customers, the economic consequences will be negative for customers.[79]

D. AI Act and the Risk Based Approach

34 The AI Act lays down "harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union"[80] and aims to bring a "legal framework for trustworthy AI".[81] The specific objectives mainly focus on the safety of AI systems. On one hand, there are economic objectives such as strengthening the single market with safe AI and on the other hand, there are objectives related to the fundamental rights and Union values.[82]

35 The responsibilities in the AI Act differ according to the roles and the risk levels. Therefore, it is important to identify the roles of e-commerce companies to find out to what extent the AI Act applies to them. If the companies develop their own AI systems, they shall be considered providers.[83] If they only use AI systems that are developed by others, they shall be considered deployers.[84]

36 If an e-commerce company is a provider and places on the market or puts into service AI systems in the Union[85] or the "output produced by the system is used in the Union",[86] it will be subject to the AI Act. If it is a deployer, it must be "located within the Union"[87] or the "output produced by the system" must be "used in the Union".[88]

37 Chapter II explains the prohibited AI practices and the conditions and exemptions for these prohibitions (unacceptable risks). Chapter III covers the high-risk AI systems and explains the classification of AI systems as high risk (Section 1), requirements for high-risk AI systems (Section 2), obligations of providers and deployers of high-risk AI systems and other parties (Section 3), notifying authorities and notified bodies (Section 4), standards, conformity assessment, certificates, registration (Section 5). Chapter IV brings transparency obligations for providers and deployers of certain AI systems. The "certain AI systems" here is what we may see as a "limited risk" group. Finally, Chapter X introduces a mechanism to formulate codes of conduct for minimal or no-risk groups, which it mentions as "AI systems other than high-risk AI systems".[89] It is possible to address the four levels of risks in the AI Act as "unacceptable risk, high risk, limited risk, and minimal or no risk" AI systems.[90]

38 Section D.I will examine the manipulative practices and social scoring of the prohibited practices from the e-commerce perspective to find out whether e-commerce activities might be prohibited under the AI Act. To evaluate whether using AI in e-commerce is safe enough not to be subject to high-risk AI obligations of the AI Act, Section D.II will then compare the risks of e-commerce activities with the AI Act's criteria in Article 7(2) to be considered a high-risk AI system. Sections D.III and D.IV will explain the meaning of limited and minimal risk groups for e-commerce.

I. Unacceptable Risk AI Systems: Prohibited Practices

39 The AI Act prohibits AI practices that could be classified under the unacceptable risk group. These practices include subliminal techniques,[91] exploiting

78 Zuiderveen Borgesius, Poort, 'Online Price Discrimination and EU Data Privacy Law' (n 16), 357

79 *Ibid*, 354

80 AI Act art 1(2)(a)

81 AI Act Proposal Explanatory Memorandum, 1

82 AI Act Proposal Explanatory Memorandum, 3

83 AI Act art 3(3)

84 AI Act art 3(4)

85 AI Act art 2(1)(a)

86 AI Act art 2(1)(c)

87 AI Act art 2(1)(b)

88 AI Act art 2(1)(c)

89 AI Act art 95(1)

90 European Commission, 'Regulatory framework proposal on artificial intelligence' (Shaping Europe's digital future, last update 20 June 2023) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 12 October 2023

91 AI Act art 5(1)(a)

vulnerable groups,[92] biometric categorisation systems based on special categories of personal data,[93] social scoring,[94] real-time remote biometric identification in publicly accessible spaces for law enforcement purposes,[95] risk assessments for criminal activities,[96] facial image scraping from CCTV footages,[97] and emotion inferences in workplace and education institutions.[98] The prohibited practices that are most likely to occur in e-commerce are the manipulative practices in Articles 5(1)(a) and 5(1)(b) and social scoring in Article 5(1)(c). These prohibited practices create risks in relation to manipulation and discrimination. The other prohibited practices in Chapter II of the AI Act will not be examined here.

1. Manipulative Practices

a.) Subliminal Techniques

40 The first prohibited practice in Article 5(1)(a) is the "placing on the market, putting into service or use of an AI system that deploys subliminal techniques". Article 5(1)(a) requires using "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques with the objective to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision", and significant harm to occur or be likely to occur because of this use.

41 As explained in section C.I, manipulation can be seen often in e-commerce activities, especially in marketing. Manipulative practices can be to hide some information from customers, to use misleading language, to mislead customers with "fake countdown timers".[99] However, not every technique to sell a product is manipulation and not every manipulation is covered by the prohibition in the AI Act. In order to consider a technique manipulation in the sense of the AI Act, subliminal techniques must be applied to sell a product.

42 In the Proposal, the article required the intention to materially distort a person's behaviour in a manner that causes or is likely to cause harm when using subliminal techniques.[100] However, in practice, distorting a person's behaviour is possible, even if it is not intentional. Therefore, this is changed in the Adopted Text to include the unintentional cases.

43 Subliminal techniques are not defined in the text. In the recitals, they are explained as techniques that affect autonomy or decision-making abilities even though they cannot be perceived as subliminal techniques, or they cannot be controlled even though perceived.[101] In e-commerce, such extreme techniques are not likely to be used in practice.

44 The text excludes some important situations from the scope of the article. Some manipulation techniques can still cause serious harm even if they are not subliminal. Companies might use manipulation techniques that customers can perceive. They might send the customers timed advertisements when customers are vulnerable and more likely to buy a certain product. This may be left to other legislation such as the Unfair Commercial Practices Directive in accordance with the intentions of the AI Act that aims to be not too restrictive, but it is a weak part of it to regulate only some of the manipulative practices and not regulate the rest, which may cause the same amount of harm.

45 Another condition in the article is that the subliminal technique used must cause significant harm. Manipulation techniques can have an impact on people's decision-making, causing them to buy products that they would not normally buy, or to buy more than they intended, and overspend. However, it is not clear how to measure the degree of significant harm. Whether the damage is serious enough to fall within the scope of the article must be assessed on a case-by-case basis. In cases where all these conditions are met, this practice will be prohibited. The article is very limited because it contains very difficult and specific conditions to meet, and it does not seem very likely to have all the conditions in these provisions met at the same time.[102] Therefore, this article will not be likely to

92 AI Act art 5(1)(b)

93 AI Act art 5(1)(g)

94 AI Act art 5(1)(c)

95 AI Act art 5(1)(h)

96 AI Act art 5(1)(d)

97 AI Act art 5(1)(e)

98 AI Act art 5(1)(f)

99 European Commission, 'Consumer protection: manipulative online practices found on 148 out of 399 online shops screened' (European Commission, 30 January 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 12 October 2023

100 AI Act Proposal art 5(1)(1)

101 AI Act recital 29

102 Michael Veale, Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021)

apply to e-commerce practices.

b.) Vulnerable Groups

46 Article 5(1)(b) protects a person or a specific group of persons such as children, disabled persons or in a specific social or economic situation and prohibits the use of an AI system that exploits the vulnerabilities of these groups. Similar to Article 5(1)(a), the requirement of intent to materially distort the behaviour is changed in the Adopted Text and now the article covers also unintentional distortion. The Proposal did not include specific social or economic situations. They are included among the disadvantaged groups in the Adopted Text.

47 Situations like Article 5(1)(b) are more likely to be seen in practice. For its applicability is sufficient to exploit any vulnerability of a specific group of persons. For its application, the use of subliminal techniques is not required. In e-commerce, manipulation techniques to sell products to children, for example, will be covered in the article. Moreover, since the article includes specific social and economic situations, manipulating people with certain addictions by discovering their addictions through their purchasing histories may be in the scope of the article if these amendments are approved.

48 Again, the manipulation must cause or be likely to cause significant harm. Since the article states that the person who will be harmed can be a person other than the person from the specific group, it will be a prohibited practice if, for example, the families of children who have faced this harm or are likely to face it. It is not clear what will be considered significant harm. However, the article is important for e-commerce since it covers harms that are likely to arise from e-commerce while still preventing insignificant risks from being included unnecessarily. Similar to Article 5(1)(a), practices must be considered case-by-case basis.

c.) Complementary Aspect of the AI Act

49 Some of the manipulative practices might already be covered by other EU legislation. The Unfair Commercial Practices Directive prohibits materially distorting,[103] misleading[104] or aggressive practices.[105] In addition to those, Annex I of the Directive lists the commercial practices that are prohibited under all circumstances. For example, Annex I Article 7 prohibits "falsely stating that a product will only be available for a very limited time" time which may trigger impulsive buying. The AI Act states in the recitals that the AI Act's prohibitions of manipulative techniques are complementary to the prohibitions of the Unfair Commercial Practices Directive, which its prohibitions apply regardless of whether AI is used.[106] Moreover, by giving the example of advertising, it is stated that "common and legitimate commercial practices" that comply with the applicable law will not be considered harmful manipulative AI practices.[107] Therefore, in Articles 5(1)(a) and 5(1)(b), the AI Act mostly prohibits activities that are already prohibited.

2. Social Scoring

50 Article 5(1)(c) concerns social scoring. For the AI system to be prohibited under the article, both the conditions leading to the social score and the results caused by the social score must meet the criteria listed in the article. First, a social score must be created by evaluating or classifying a natural person's "social behaviour or known or predicted personal or personality characteristics" over a certain period of time. Then, this social score must lead to detrimental or unfavourable treatment by using the data in an unrelated context compared to what it was originally collected for or by using the data in an unjustified or disproportionate manner considering the social behaviour.[108] Therefore, social scoring that does not lead to these results is not prohibited.

51 Social scoring includes credit scores. This is the creation of a financial trustworthiness score about natural persons by evaluating their actions in different contexts.[109] However, scoring in the broad

22 Computer Law Review International 97, 98

103 Unfair Commercial Practices Directive art 5(2)(b)

104 Unfair Commercial Practices Directive arts 6, 7

105 Unfair Commercial Practices Directive art 8

106 AI Act recital 29

107 *Ibid*

108 AI Act art 5(1)(c)

109 'Social scoring systems: current state and potential future implications' (Kaspersky Daily) <https://www.kaspersky.com/blog/social-scoring-systems/> accessed 13 October 2023

sense is not limited to this, and it is possible to collect information about a person in various contexts and evaluate them in another context.[110] The AI Act does not define social scoring in the text. However, it is defined in the recitals as "such AI systems evaluate or classify natural persons or groups thereof based on multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time."[111]

52 In e-commerce, scoring in the traditional sense would be the case where customers are denied access to certain services or charged a higher price for them. For example, if customers cannot see some products on the website according to the score created about them, this will be considered a traditional scoring. Scoring can be commonly used in e-commerce through predictive analytics and consumer scores. E-commerce companies may have lawfully obtained data about customers such as name, address, age, and gender. In addition, they can make inferences about customers leading to consumer scores using predictive analytics. While the data that can be collected about the customers in physical stores are limited, much more data which are not limited to the shopping itself can be collected about them in the case of online shopping.[112]

53 In order to predict whether the customer will buy a certain product, "clickstream data", "customer demographics" and "historical purchase data" can be analysed.[113] When the data collected about customers are combined with other data, inferences can be made about them. This may cause data protection, privacy, and autonomy problems.[114] Even when the collected and processed data are not particularly sensitive, the inferences made based on these data can relate sensitive personal data. For example, buying certain foods or not shopping on certain days due to religious reasons may lead to inferences about religion.[115] Using the inferences about a person's religion in another context, for a detrimental or unfavourable treatment, will fall under Article 5(1)(c)(i). It is not clear what counts as a different context in the article. While the consequences of making inferences about a person's religion might be problematic within the scope of privacy or discrimination law, for example, showing this person similar products purchased by this group on the same website will not be a different context in the sense of the AI Act. However, it is not clear whether the context will be considered different if this inference is used on another e-commerce website. In any case, the use of this inference in another sector such as health or education and detrimental or unfavourable treatment based on this inference or using the inferences from different sectors in e-commerce will fall within the scope of Article 5(1)(c)(i).

54 Moreover, since predictive analytics can divide people into certain groups, some people may not be able to take advantage of economic benefits.[116] Some discounts may not be shown to certain groups, or people may be subjected to price discrimination because of a prediction. However, although the restriction of access to certain products and the fact that they cannot see them at all can be considered within the scope of Article 5(1)(c)(ii), the fact that they cannot benefit from some discounts cannot be considered as a disproportionate treatment.

55 It is possible for e-commerce activities to meet the conditions of both Article 5(1)(c)(i) and 5(1)(c)(ii) since companies often make inferences about customers and create scores about them. This article in the Proposal was not applicable to e-commerce as it did not include private actors. However, this approach was criticised. For example, EDPB and EDPS stated that the imposition of such specific requirements for prohibited AI systems was an approach that possibly limits the practical effectiveness of the AI Act.[117] They suggested that the prohibition should cover any type of social scoring since it can also be conducted by private companies.[118] This is changed in the Adopted Text to include private actors as well. Therefore, the prohibition is now applicable to e-commerce activities if the conditions in the article are met.

110 *Ibid*

111 AI Act recital 31

112 Dirk Van den Poel, Wouter Buckinx, 'Predicting online-purchasing behaviour' (2005) 166 European Journal of Operational Research 557, 557

113 *Ibid*, 561-566

114 Shaun B. Spencer, 'Privacy and Predictive Analytics in E-Commerce' (2015) 49 New England Law Review 629, 640

115 Tal Z. Zarsky, 'Understanding Discrimination in the Scored Society' (2014) 89 Washington Law Review 1375, 1395

116 Spencer (n 114), 629

117 EDPB-EDPS Joint Opinion (n 50), para 28

118 *Ibid* para 29

II. High Risk AI Systems

1. Is E-Commerce High Risk According to the AI Act?

56 A large part of the AI Act is allocated to the rules regarding high-risk AI systems. High-risk AI systems can be examined in two main parts: those with health and safety risks (Article 6(1)) or those with fundamental rights risks (Article 6(2)).[119] For an AI system to be considered a high-risk AI system according to Article 6(1), the AI system must be a safety component of a product or a product itself, that is covered by the Union harmonisation legislation listed in Annex II and is required to undergo a third-party conformity assessment. Article 6(2) states that "in addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk".[120]

57 As a result of the classification of an AI system as high risk, the AI systems will need to comply with the requirements such as the risk management system,[121] data and data governance,[122] technical documentation,[123] record keeping,[124] transparency,[125] human oversight,[126] accuracy, robustness and cybersecurity.[127]

58 Since Article 6(1) and Annex II refer to the list of Union harmonisation legislation and relate to product safety, it is not relevant for e-commerce. Article 6(2) and Annex III relate to fundamental rights. It appears that the risks of e-commerce activities are not considered high risk under Annex III of the AI Act since Article 6(2) refers to specific areas such as biometrics, critical infrastructure, education and vocational training, employment, access to essential private services[128] and public services, law enforcement, border control management and administration of justice.

59 The Commission can adopt delegated acts and update the list in Annex III according to Articles 7 and 97. However, it can only add the AI systems intended to be used in the already existing areas mentioned above, and it cannot add any new areas to this list.[129] The sub-areas can be updated, but only if they involve equivalent or greater risk to health and safety or fundamental rights than already existing ones.[130] The criteria to be applied to compare these risks are specified in Article 7(2).

60 Since the high-risk AI systems are determined in the Annexes of the AI Act and e-commerce is not included in them, most of the AI systems used here are out of scope. However, as explained in Section C, e-commerce activities can also pose serious risks. Section D.II.2 will analyse whether these risks are comparable to other high-risk systems in the AI Act, and it will use Article 7(2) for this purpose.

2. Should E-Commerce Be Considered High Risk?

61 In order to compare the risks of e-commerce to the high-risk AI systems in Annex III, the risks existing in this sector need to be examined from the perspective of Article 7(2). Since the list in Annex III is exhaustive and it is not possible to add new areas to the list, the comparison within the scope of Article 7(2) will only be made to assess whether the risks of using AI in e-commerce *should be* classified as high risk or not. The criteria in Article 7(2) are examined below, following the order in the article. The issues considered as risks in e-commerce may have already been covered by Union legislation. In this case, According to Article 7(2)(k), the Commission will evaluate all these factors together and will not make any amendments if it considers that sufficient

119 AI Act Proposal Explanatory Memorandum, 13

120 AI Act art 6(2)

121 AI Act art 9

122 AI Act art 10

123 AI Act art 11

124 AI Act art 12

125 AI Act art 13

126 AI Act art 14

127 AI Act art 15

128 AI Act Recital 58 gives the examples of using creditworthiness and credit scores. These can be used in e-commerce, such as payments with instalments or buy now pay later systems. However, it should also be evaluated whether e-commerce can be considered essential. Essential private services are not defined in the text. It might be possible for e-commerce to be considered high-risk if some platforms become very dominant and considered essential in the future, and if AI is used to access them. For now, it is not likely for e-commerce to be considered high-risk for being used in access to essential private services.

129 AI Act art 7(1)(a)

130 AI Act art 7(1)(b)

redress mechanisms exist.

62 First, the intended purpose and the extent of the use of the AI system are considered.[131] Even though AI can also be used to provide convenience to customers, it is usually primarily intended for the benefit of businesses. The purposes of companies of using the AI systems can change as explained in Section B. Therefore, it is not possible to make a general assessment of the use of AI in e-commerce. The extent of the risks of AI systems must be found based on each application. Different implementations of each system, the algorithms, and the customer data used may change this evaluation.

63 "The nature and amount of data processed and used by the AI system" are also considered.[132] The article emphasises special categories of data since greater use of such data increases the risks to fundamental rights. In e-commerce, special categories of data can both be used and inferred from other data and this may pose risks to fundamental rights.

64 The level of autonomy of AI systems and of people over the AI system are considered.[133] This evaluation depends on the AI system used and the company itself. For example, while the risks may be less on a website of a company selling its own products and visited by fewer users, it may not be as easy for larger platforms with many users to provide human oversight to the decisions or recommendations made by AI.

65 Then, harm to health and safety and the adverse impact on fundamental rights are considered. Here, both previously encountered harms[134] and potential harms[135] are taken into account. As explained above, the use of AI in e-commerce may create risks, especially manipulation and discrimination. In addition, data protection problems may arise due to the nature of AI using a great amount of data. As it was mentioned, the AI Act imposes detailed conditions that are not always possible to meet at the same time. For example, manipulating a person can be done without using subliminal techniques. In this case, this practice will remain unregulated under the AI Act. However, it might be more appropriate to consider these practices as high-risk practices and take precautions accordingly.

66 Moreover, collecting personal data through information brokering and using it for advertising purposes may also cause data protection problems. Profiles of people created by data brokers by collecting and combining information from various sources may cause some problems[136] such as assessing the credibility of people based on data other than financial data ("credit scoring"),[137] inaccuracies of the profiles if the source information is incorrect or discrimination.[138] Practices such as Real Time Bidding (RTB) may cause privacy breaches while collecting data in the background and without people being aware of it.[139] In addition to the privacy breaches, RTB is also dangerous because even if people have consented to the further use of their data under the GDPR, they may not fully understand the scope of this further use.[140]

67 Another point to consider is the extent of the dependency of the people affected by these practices on the outcomes reached by AI, and the possibility of opt-out from these outcomes.[141] The article puts focus on practical reasons for this opt-out option as well. Customers may have to accept some conditions while shopping online to see the website, or purchase something. For example, while shopping online, cookies on the website may be rejected, except for essential cookies. However, this will still not prevent the collection of some data about the customer. While the collection of this data may not be in itself unlawful according to the data protection rules, practices such as profiling and making inferences about customers can lead to unlawful results such as discrimination. Moreover, sometimes technical impossibilities can cause problems. For example, in RTB, once the data are shared with third parties,

131 I Act arts 7(2)(a), 7(2)(b)

132 AI Act art 7(2)(c)

133 AI Act art 7(2)(d)

134 AI Act art 7(2)(e)

135 AI Act art 7(2)(f)

136 Shivangi Mishra, 'The dark industry of data brokers: need for regulation?" (2021) 29 International Journal of Law and Information Technology 395, 399

137 *Ibid*,399

138 *Ibid*, 401

139 Johnny Ryan, 'The Biggest Data Breach, ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe' (Irish Council for Civil Liberties, 16 May 2022) <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf> accessed 13 October 2023

140 IAB Europe, IAB Tech Lab, 'GDPR Transparency and Consent Framework' <https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#About-the-Framework> accessed 13 October 2023

141 AI Act art 7(2)(g)

technically it is not possible to restrict the use of these data.[142] It can be argued that it is not compulsory for the customer to shop online if these conditions are not acceptable. However, especially today, it is not practically reasonable to expect this from customers, and customers may tend to accept these conditions without reading them carefully or considering the consequences.

68 The position of the affected person "in relation to the user of the AI system" is also a point to be considered, especially in terms of "imbalance of power, or potentially harmed or suffer an adverse impact" "due to status, authority, knowledge, economic or social circumstances, or age".[143] In e-commerce, there is a "power imbalance" between customers and sellers, both economically and in terms of knowledge regarding the sale.[144] The customer is in a more vulnerable position than the seller and this can affect the autonomy of the customers in online shopping. The price and product information presented to customers affects their online purchasing behaviours.[145] Not only the information presented but also "*how* and *when* it is displayed" can influence the behaviour of customers and can be used to manipulate them.[146]

69 Whether the "outcome produced with an AI system is easily corrigible or reversible" is also a point to be evaluated.[147] It is stated in the article that the outcomes affecting the "health, safety, fundamental rights shall not be considered as easily reversible".[148] Here, manipulation and its effects on mental health can be considered in terms of health and safety. The use of manipulation in a way that leads to making customers spend more money than they intend to, and these material consequences, therefore, can be considered easily reversible. Nevertheless, in e-commerce, it is more likely to encounter risks such as discrimination and privacy than health and safety risks. These issues should also be evaluated separately according to each AI system applied and the outcomes it produces.

70 Finally, the extent to which existing Union legislation protects against these risks and redress mechanisms must be evaluated.[149] Claims for damages are excluded from the assessment of the "effective measures of redress".[150] For example, in data protection and privacy issues, the GDPR gives data subjects the right to compensation.[151] However, it also provides protection with the rights of the data subject[152] such as the right to rectification, right to erasure, and right to restriction of processing. The effective redress under the AI Act Article 7(2)(k) refers to rights. Whether this is an effective redress against the outcome reached by the AI system may change case by case. For e-commerce, each case will be different depending on whether this redress is effective or not. If the redress is not effective, the practice would fall under the scope of high risk, considering the other conditions as well.

71 Regarding the discrimination risks, even though the non-discrimination law provides some solutions for them, there are cases that these risks may not be covered.[153] AI systems can discriminate based on different characteristics that are not protected in non-discrimination law.[154] For example, prices that customers see may differ according to the browser used.[155] Therefore, current legislation may not always provide effective protection against the use of AI.

72 However, whether the AI Act must provide extra protection must be evaluated by examining all these conditions in Article 7(2) together. Most AI uses in e-commerce fall outside the scope of high-risk according to these criteria, and it would not be proportionate to place e-commerce entirely within the scope of high-risk. However, there may be cases where AI applications that cause serious manipulation, discrimination or data protection risks meet all the criteria of Article 7(2) and therefore should be considered within the scope of high-risk AI systems. Furthermore, it is appropriate to consider some practices such as manipulation and social scoring, which do not meet all the criteria to be included in the scope of prohibited practices, within

142 IAB Europe, IAB Tech Lab (n 140)

143 AI Act art 7(2)(h)

144 Lippi and others (n 15), 171

145 Eliza Milk, 'The erosion of autonomy in online consumer transactions' (2016) 8 Law, Innovation and Technology 1, 1

146 *Ibid*, 2

147 AI Act art 7(2)(i)

148 AI Act art 7(2)(i)

149 AI Act art 7(2)(k)

150 AI Act art 7(2)(k)(i)

151 GDPR art 82

152 GDPR Chapter III

153 Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (n 16), 20

154 *Ibid*, 35

155 *Ibid*, 35, 36

the scope of high-risk.

III. Limited Risk AI Systems ("Transparency Obligations for Providers and Deployers of Certain AI Systems"[156])

73 Article 50 regulates transparency obligations for providers and deployers of certain AI systems. What obligations e-commerce companies must comply with will vary depending on whether they develop their own AI systems or use AI systems developed by third parties.

74 Article 50(1) brings an obligation of disclosure to providers. If an AI system is "intended to directly interact with natural persons" the providers must inform the natural persons that this is an AI system. However, if it is obvious from the "circumstances and the context of use", disclosure will not be necessary.[157] Chatbots are AI systems that interact with natural people. Many e-commerce companies can use chatbots on their websites. However, the disclosure responsibility is on the provider. If e-commerce companies use the chatbots that they design on their own, they must design them in a way that the natural persons interacting with these chatbots are aware that they are interacting with an AI system. In case e-commerce companies are using chatbots developed by third parties and the developers of the chatbot have failed to design it in this way, e-commerce companies are not obliged to inform the natural persons as deployers. However, since the purpose of the article is to protect natural persons, it may be good practice for companies to not use chatbots that are not compliant with this obligation.

75 Article 50(3) states that "deployers of an emotional recognition system or biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto". Veale and Zuiderveen Borgesius noted that while it is not clear what this provision adds to the existing data protection obligations, the intention of the article might be to apply to AI systems that do not process personal data as well.[158]

76 E-commerce companies might use emotion recognition systems in their activities. Techniques such as sentiment analysis, which are used to analyse people's opinions about a subject,[159] can work without processing personal data. For example, customer reviews on websites might be analysed to find out a positive or negative opinion about a particular product without using any personal data of the customer. However, whether these techniques fall within the scope of emotional recognition under the AI Act is not clear.

77 Article 50(4) also brings obligations for the deployers and relates to deep fakes. Deployers are obliged to disclose if an "image, audio or video content constituting a deep fake" is "artificially generated or manipulated".[160] Article 50(2) brings a similar disclosure obligation to providers as well.[161] However, this article does not mention deep fakes and covers "synthetic audio, image, video or text content".[162] The contents relating to these two obligations are mentioned as "synthetic"[163] and "falsely appear to a person to be authentic"[164] in the recitals. In the context of e-commerce, generated content within the meaning of Article 50(2) is more likely to be used in practice. For example, if the images of the products sold are AI-generated, this should be disclosed by the company. Such a situation may not occur very often in practice unless it is about underdeveloped prototypes or AI-generated images showing how clothes would fit customers. Nevertheless, whether they are providers or deployers, e-commerce companies have various disclosure obligations under Articles 50(2) and 50(4).

78 This article will be applied in addition to the high-risk requirements and obligations in Chapter III.[165] Although it is not specified in the article, it is clear that the AI systems mentioned in this article cannot be used in any way if they fall within the scope of the AI Act's prohibited practices.

156 AI Act Chapter IV

157 AI Act art 50(1)

158 Veale, Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (n 102), 107

159 Pansy Nandwani, Rupali Verma, 'A review on sentiment analysis and emotion detection from text' (2021) 11 Social Network Analysis and Mining 81, 81

160 AI Act art 50(4)

161 AI Act art 50(2)

162 *Ibid*

163 AI Act recital 133

164 AI Act recital 134

165 AI Act art 50(6)

IV. Minimal / No-Risk AI Systems

79 AI systems other than the above-mentioned risk groups are considered as minimal / no risk and there is no obligation for them under the AI Act. The AI systems used in e-commerce activities that do not fall under the scope of the prohibited practices, high-risk or limited risk AI systems, they will fall under the minimal / no-risk scope. Other EU legislation such as data protection, non-discrimination, and consumer protection law will continue to be applied to these AI systems. However, the AI Act does not impose any additional obligations on them.

80 The AI Act introduces a mechanism to drawing up and voluntary application of Codes of Conduct in Chapter X for AI systems other than those classified as high-risk. This is to encourage the voluntary implementation of the some or all of the requirements in Chapter III, Section 2, relating to high-risk AI systems.[166] Article 95(3), states that codes of conduct can be drawn up by both individual providers or deployers and the organisations representing them, and deployers and interested stakeholders can be involved in this process.

81 The implementation of voluntary codes of conduct will entail large numbers of obligations for e-commerce companies. In Chapter III, Section 2, obligations for high-risk AI systems are specified. These are detailed obligations regarding risk management system, data and data governance, technical documentation, record-keeping, transparency and provision of information to deployers, human oversight, and accuracy, robustness and cybersecurity. It may not be realistic to expect e-commerce companies to comply with these extra rules that are not mandatory. Adding these obligations to those that already must be complied with can be a heavy burden for companies, both financially and in terms of resources. However, complying with them may put them in a better position in terms of public prestige and credibility than other companies that choose not to implement voluntary codes of conduct.

E. Conclusion

82 AI has many benefits and is therefore often used in e-commerce. With the help of AI, companies can have abundant and accurate information about their customers and the market, make predictions and adjust their actions accordingly. AI enables companies to be efficient, reduce workload and increase profits. However, the use of AI may also cause some risks related to transparency, human control, and accountability.[167] The two most serious risks that the use of AI may bring are manipulation and discrimination.

83 The AI Act is an important piece of legislation by the EU in this area and it has adopted a risk-based approach. According to the risk-based approach, the AI Act prohibits some practices, imposes obligations about some AI systems, or leaves some of them unregulated. The applicability of the AI Act to e-commerce activities is determined according to these risk levels. This article researches the following questions: *To what extent do the provisions of the AI Act apply to e-commerce companies that use AI? To what extent is this in line with the objectives of the AI Act, considering the risks in relation to the use of AI for e-commerce?*

84 The applicability of the AI Act in e-commerce depends on the AI techniques used, and the role of the e-commerce company as a provider or deployer. The prohibited practices in the AI Act are for both providers and deployers. The prohibited practices that might relate to e-commerce activities in the AI Act are the subliminal techniques in Article 5(1)(a), vulnerable groups in 5(1)(b) and social scoring in 5(1)(c). However, since Article 5 has many conditions that are difficult to meet at the same time, it will be unlikely for e-commerce activities to be in the scope of the article. Furthermore, practices that fulfil all those conditions may also be prohibited under existing law such as the Unfair Commercial Practices Directive. Nevertheless, the practices must be evaluated on a case-by-case basis to see whether they would be prohibited or not.

85 According to the AI Act, AI systems that are used in e-commerce are not high-risk AI systems. However, these AI systems may still cause serious risks. The AI Act lists high-risk AI systems in specific areas, and it is not possible to add new areas to the existing areas. This approach excludes AI systems that may pose significant risks. Although not all use of AI in e-commerce poses risks serious enough to be considered high-risk according to the AI Act, some applications may pose serious risks enough to meet the criteria in Article 7(2), especially in practices such as manipulation and social scoring. If the AI system in question is not a high-risk or limited-risk AI system and does not fall within the scope of prohibited practices only because it does not meet one of the many conditions in the article, it can be left completely unregulated under the AI Act. For example, a manipulative practice may not be considered a prohibited practice only because it does not use subliminal techniques. Similarly, not all practices that lead to risks may be prohibited

166 AI Act art 95(1)

167 EDPB-EDPS Joint Opinion (n 50), para 3

under the Unfair Commercial Practices Directive. Regulating such practices at least to a certain degree would provide better protection by the AI Act against these risks. Furthermore, such regulation would complement existing rules by imposing obligations on the AI systems themselves, instead of only on the use of such systems in specific situations.

86 Article 52 regulates transparency obligations for certain 'limited risk' AI systems. Obligations related to these vary depending on whether the e-commerce company is a provider or a deployer. There are no obligations for the AI systems that are considered minimal or no-risk AI systems. However, companies can apply the obligations for high-risk systems in the AI Act by implementing codes of conduct. This may increase their reliability and give them a competitive advantage. Voluntary compliance with these obligations will be beneficial in mitigating some of the risks of using AI in e-commerce. However, these are serious risks that should not be left to companies' discretion and instead of voluntary compliance, addressing them somewhere else in the AI Act could be a better approach.

87 The AI Act leaves a regulatory gap in the use of AI in e-commerce, considering the risks. The two important objectives of the AI Act are product safety and fundamental rights. However, the AI Act seems to concentrate more on product safety. AI systems in e-commerce are left largely unregulated, even though they can also create serious risks comparable to those of high-risk systems. The AI Act could be more effective if it did not exclude such important risks and had a larger scope.