Chatbots by business vis-à-vis consumers: A new form of power and information asymmetry

Zanda Davida[1,*]

[1] University of Latvia, Faculty of Law, 19 Raina Blvd, Riga, Latvia. Turiba University, Faculty of Law, 68 Graudu St., Riga, Latvia

Abstract

Research background: The first notable early chatbots were created in the sixties, but the growing use of artificial intelligence (AI) has powered them significantly. Studies show that basically chatbots are created and used for purposes by government and business, mostly in consumer service and marketing. The new Proposal of the Artificial intelligence act aims to promote the uptake of AI and address the risks associated with certain uses of such technology. However, the act contains only minimum transparency obligation for some specific AL systems such as chatbots.
Purpose of the article: In light of this issue, the article aims to discuss how existing European Union (EU) consumer law is equipped to deal with situations in which the use of chatbots can pose the risks of manipulation, aggressive commercial practices, intrusion into privacy, exploitation of a consumer's vulnerabilities and algorithmic decision making based on biased or discriminatory results.
Methods: The article will analyse the legal framework, compare guidance documents and countries' experiences, study results of different consumer behavior researches and scientific articles.
Findings & Value added: The article reveals several gaps in current EU consumer law and discusses the flaws of proposing legislation (particularly the Proposal for an Artificial intelligence act) regarding relations between business and consumers.

Keywords: *Chatbot; Artificial Intelligence, Consumer Law; Manipulation*

JEL Classification: *K29; K39; M31; M37; M38*

1 Introduction

The advances of digitalization come with important benefits for consumers as they can access a wider range of goods and services in a more convenient manner. However, as consumers increasingly transact and interact online, they are also exposed to new risks to their decision-making autonomy, privacy, and balance of power in the relationship between them and

* Corresponding author: zn05003@edu.lu.lv

businesses. In the last decade, digitalisation has developed rapidly, but the COVID-19 crisis has significantly accelerated it.

The COVID-19 crisis and the resulting restrictions have changed consumers' shopping habits. In an unexpectedly short time, many consumers have learned to buy goods online and discovered the benefits and convenience of digital services. Studies show that these consumers' habits do not change significantly even when countries remove or reduce offline shopping restrictions. Consumers willingly use personal assistants and chatbots. Conversational assistants, such as Siri (Apple), Alexa (Amazon), and Google Assistant, are ubiquitous (Bickmore et al., 2018). Social chatbots, such as Xiaolce and Replika, are increasingly popular (Skjuve et al., 2021). On one hand, these devices make consumers' lives significantly easier. They allow them to make purchases, retrieve information, make their homes smarter, etc. without much effort. At the same time, they also pose a number of economic and non-economic risks for consumers (Stucke and Ezrachi, 2017). For example, the risks of manipulation, aggressive commercial practices, intrusion into privacy, exploitation of a consumer's vulnerabilities, and algorithmic (Gal and Elkin-Koren, 2017) decision making based on biased or discriminatory results.

On 21 April 2021, the European Commission came up with the Proposal for an Artificial intelligence act (European Commission, 2021). It is the first legislative proposal that contains special rules for new technologies such as artificial intelligence (AI). The proposal sets harmonised rules for the development, placement on the market, and use of AI systems in the European Union following a proportionate risk-based approach. It proposes a single future-proof definition of AI. The emphasis in the Artificial intelligence act is on the aim to prohibit certain particularly harmful AI practices and to develop horizontal mandatory strict regulation for "high-risk" AI systems. For some specific AI systems, in particular when chatbots, personal assistants, or "deep fakes" are used, only minimum transparency obligations are proposed.

Despite the assumption that personal assistants can cause more serious harm compared to chatbots, the degree of harm suffered by consumers will depend according to the context (EUI, 2018). Therefore, the use of chatbots technically allows the use of dark patterns, aggressive un discriminatory techniques, which can cause just as serious harm as personal assistants. As the legal aspects of chatbots techniques by businesses have not been extensively studied, the article put forward for analysis the technological practice of chatbots.

The article aims to analyse how existing EU consumer law, including the Proposal for an Artificial intelligence act is equipped to deal with situations in which the use of chatbots can pose the risks of manipulation, aggressive commercial practices, intrusion into privacy, exploitation of a consumer's vulnerabilities and algorithmic decision making based on biased or discriminatory results. Accordingly, this paper is structured as follows: Chapter 2 gives an overview of the potentials use of chatbots as AI technologies in consumer markets, the problematic features, and the specific risks these AI systems pose for consumers; Chapter 3 addresses the businesses liability for AI during the life cycle of chatbot and looks toward the future, asking whether current Proposal for an Artificial intelligence act can close the gaps that currently exist in European consumer law as it applies to chatbots as AI systems. In addition to such exploration, the article provides some suggestions.

2 Methods

The article will analyse the legal framework, compare guidance documents and countries' experiences, study results of different consumer behavior researches and scientific articles through the method of normative analyses of the law, as well as grammatical, teleological, systematic, analytical, deductive and inductive scientific research methods.

3 Results

The article reveals several gaps in current EU consumer law and outlines the shortcomings of the Proposal for an Artificial Intelligence Act. The author calls to develop a common framework for fair digital practices, which is bases on using the concept of consumer digital vulnerability.

4 Discussion

4.1 Use of chatbots: risks for consumers

The term “artificial intelligence” has been in use for nearly 70 years, but no universally accepted definition of AI has emerged (Bokovnya et al., 2020). There are innumerable definitions of AI in the scientific literature. Scholars tend to define the discipline differently, depending on whether they are concerned with the process (“thinking”) or outputs (“acting”), and whether they take as a threshold “being like a human”, or being “rational” (Russell and Norvig, 2016). Despite this, the Proposal for an Artificial intelligence act defines the concept of an "artificial intelligence system”. It must be acknowledged that the definition has come up well because it seeks to be as technology-neutral and future-proof as possible, taking into account the fast technological and market developments related to AI. Namely, the concept of “artificial intelligence system” is not so much based on current technological achievements, as on possible technological approaches.

The Proposal for an Artificial intelligence act refers to chatbots as specific AI systems, therefore there is no legal doubt about chatbots belonging to AI systems in the context of an Artificial intelligence act. Chatbots (also known as a talkbot, chatterbot, bot, IM bot, interactive agent, artificial conversational entity or virtual assistants, digital assistants, digital agents) are software agents that provide access to services and information through interaction in the users’ everyday language through text or voice (Brandtzaeg and Følstad, 2018). Chatbots are divided into several types according to their ability to communicate with humans. Nowadays a dominant type of chatbots in the market are the so-called rule-based chatbots whose role is limited to operating only in the range of specific, closed databases (Kaczorowska-Spychalska, 2019). The development trends of practice of using chatbots and technological advances show that the potential of chatbots is much more significant. For example, social chatbots are designed to act as social actors (Ho et al., 2018) where users may form social-emotional relationships (Bickmore et al., 2010). The use of chatbots can pose the risks of manipulation, aggressive commercial practices, intrusion into privacy, exploitation of a consumer's vulnerabilities, and algorithmic decision making based on biased or discriminatory results. Chatbots are designed to be dynamic, able to learn and change, so businesses must also determine what boundaries to set as their chatbots evolve over time (Daughert and Wilson, 2018). Therefore, the question arises – whether the business will have the will and motivation to set red lines throughout the whole chatbots’ lifecycle?

4.2 Liability for chatbots

At this moment the fair use of chatbots is governed by the Unfair Commercial Practices Directive (UCPD) (Unfair Commercial Practices Directive, 2005). Many legal studies show that the UCPD is too narrow to sufficiently addresses the problem of dark patterns and other ways of online behavioural advertising: 1) the definition of “aggressive practices” do not cover all forms of aggressive behaviour, because asks for the presence of pressure, which is normally absent in subtle forms of nudging (Ebers, 2021); 2) the benchmarks of “average”

and "vulnerable" are too static as neither definition sufficiently reflects that businesses in the age of AI and big data analytics have the technological capacity to exploit temporary vulnerabilities and not just those caused by age, mental infirmity or credulity, as foreseen by Article 5(3) UCPD (Leczykiewicz and Weatherhill, 2018). But the biggest challenge in practice is to get information on how interfaces are working. Namely, to look in the "black box" of methods used by businesses. It is no secret that these methods are based on the consumer choice architecture (Thaler and Sunstein, 2021). Therefore, the digital consumer choice can be made irrational. AI systems, including chatbots, have the technical capacity to exploit consumer digital vulnerability and the UCPD does not deal with it.

An Artificial intelligence act should be based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions while encouraging businesses to develop them. AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being. Despite the noble aim of the Proposal, in reality, regulation will protect particularly basic EU values and fundamental human rights. Most consumer rights and personal data rights are left outside the regulatory framework of AI systems. The Proposal Paragraph 5.2 states that manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection, and digital service legislation that guarantee that natural persons are properly informed and have a free choice not to be subject to profiling or other practices that might affect their behaviour.

Therefore, the use of such AI systems as chatbots have transparency obligations to inform consumers about the fact, that they are interacting with an AI system; users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto; users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ("deep fake"), shall disclose that the content has been artificially generated or manipulated. The exploitation of consumer digital vulnerability cannot be prevented by information because digital vulnerability is based on the consumers' irrational decision making which is unfairly used by businesses. Consumers are unable to make an objective decision when their digital vulnerability is exploited, for example through dark patterns (Narayanan et al., 2020), manipulation, aggressive techniques. Therefore, neither Artificial intelligence act have a specific obligation that could effectively avoid AI systems, including chatbots caused risks of manipulation, aggressive commercial practices, intrusion into privacy, exploitation of a consumer's digital vulnerabilities, algorithmic decision making based on biased or discriminatory results, and ensure decision-making autonomy and balance of power in the relationship between consumers and businesses, nor the UCPD.

To remove the gaps in current EU consumer law, including the flaws of proposing legislation regarding relations between business and consumers in a digital environment, the EU needs to develop a common framework for fair digital practices using AI systems that includes researches of relationships between actual digital methods and civil sociality (consumers). This should be followed by more effective monitoring and the promotion of self-regulation tools such as codes of good practice.

5 Conclusions

Personalization algorithms are used to help users to handle the abundance of information online and find the content that matters to them (Thurman et al., 2019). Chatbots are a great example of this. They can bring many benefits to consumers – potentially easier and faster communication with businesses, easier access to content, goods, services, and more convenient digital solutions. However, tracking and targeting users cannot only create new

opportunities but potentially also new disparities and vulnerabilities in society, and users (Bol et al., 2020). Development of the concept of consumer digital vulnerability is still in progress because it cannot be seen only as a legal concept (Davida, 2021). compared to "vulnerable consumer" according to the UCPD. Digitalization, particularly the rise of AI, brings a new aspect to the concept of "vulnerable consumer". Each consumer can be vulnerable in its own way and that vendors have the technological capacity to exploit temporary vulnerabilities – not just those caused by age, mental infirmity, or credulity (Mik, 2016) according to Article 5 of the UCPD. The digital vulnerability arises when businesses nudge consumers to make irrational decisions by using the knowledge of consumers' choice architecture. Namely, businesses are using consumers' natural deep of decision-making process, which consumers are usually unable to influence even if they have information about the methods used by the businesses. The same nudging can be used by chatbots and that is wrong because consumers have the right to act in the trustful digital environment, which embodies a high level of consumer protection according to Article 28 of the EU Charter of Fundamental Rights.

Current EU consumer law, including an Artificial intelligence act, does not offer a legal solution to these gaps. Thereby the use of such AI systems as chatbots still can legally safely pose the risks of manipulation, exploitative practices, and exploitation of a consumer's digital vulnerabilities, because authorities have an inefficient legal basis to combat such practice. Namely, authorities can use the UCPD, which is too narrow for this new digital practice, or in the future more likely will have the possibility to use an Artificial intelligence act, which put forward transparency obligations. Unfortunately, providing more information to consumers fails to reduce consumer digital vulnerability in the context of this discussion.

Therefore, the EU needs to develop a common framework for fair digital practices, which is bases on using the concept of consumer digital vulnerability. The best place for this regulation is the UCPD, which should be complemented by the concept of consumer digital vulnerability. For effective monitoring, the regulation needs to give the ability (even the obligation) for authorities to receive information and do research on how interfaces are working, and how they interact with civil sociality (consumers). Namely, to look in the "black box" of AI systems life cycle. Also, the promotion of self-regulation tools such as codes of good practice is welcome too.

References

1. Brandtzaeg, P. B., & Følstad, A. (2018). Chatbots: Changing user needs and motivations. *Interactions*, *25*(5), 38–43.
2. Bickmore, T. W., Mitchell, S. E., Jack, B. W., Paasche-Orlow, M. K., Pfeifer, L. M., & O'Donnell, J. (2010). Response to a relational agent by hospital patients with depressive symptoms. *Interacting with Computers*, *22*(4), 289–298.
3. Bickmore, T. W., Olafsson, S., O'Leary, T. K., Asadi, R., Rickles, N. M., & Cruz, R. (2018). Patient and consumer safety risks when using conversational assistants for medical information: An observational study of Siri, Alexa, and google assistant. *Journal of Medical Internet Research*, *20*(9), 1–13.
4. Bokovnya, A. Y., Begishev, I. R., Khisamova, Z. I., Narimanova, N. R., Sherbakova, L. M., & Minina, A. A. (2020). Legal approaches to artificial intelligence concept and essence definition. *Revista San Gregorio*, (41), 115–121.
5. Bol, N., Strycharz, J., Helberger, N., van de Velde, B., & de Vreese, C. H. (2020). Vulnerability in a tracked society: Combining tracking and survey data to understand who gets targeted with what content. *New Media & Society*, *22*(11), 1996–2017.

6. Ebers, M. (2021). Liability for artificial intelligence and EU consumer law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *12* (2021), 204–220.
7. Gal, M. S., & Elkin-Koren, N. (2017). Algorithmic consumers. *Harvard Journal of Law & Technology*, *30*(2), 309–313.
8. Ho, A., Hancock, J., & Miner, A. S. (2018). Psychological, relational, and emotional effects of self-disclosure after conversations with a chatbot. *Journal of Communication*, *68*(4), 712–733.
9. Kaczorowska-Spychalska, D. (2019). How chatbots influence marketing. *Management-Poland, 23*(1), 251–270.
10. Mik, E. (2016). The erosion of autonomy in online consumer transactions. *Law, Innovation and Technology*, *8*(1), 34.
11. Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar M., (2020). Dark patterns: Past, present, and future. *Communications of the ACM*, *69*(9), 42–47.
12. Skjuve, M., Følstad, A., Fostervold, K. I., & Brandtzaeg, P. B. (2021). My chatbot companion - a study of human-chatbot relationships. *International Journal of Human-Computer Studies*, *149*, 1–14.
13. Stucke, M. E., & Ezrachi, A. (2017). How digital assistants can harm our economy, privacy, and democracy. *Berkeley Technology, 32*, 1239–1300.
14. Thurman, N., Moeller, J., Helberger, N., & Trilling, D. (2019). My friends, editors, algorithms, and i examining audience attitudes to news selection. *Digital Journalism*, *7*(4), 447–469.
15. Daugherty, P., & Wilson, H. (2018). *Human + Machine. Reimagining Work in the Age of AI*. Harvard Business Review Press, Boston, Massachusetts.
16. Leczykiewicz D., & Weatherhill S. (Ed.). (2018). *The Images of the Consumer in EU Law.* Oxford/Portland, Hart Publishing.
17. Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson Education Limited.
18. Thaler, R. H., & Sunstein, C. R., (2021). *Nudge: The Final Edition.* Penguin Book.
19. Davida, Z., (2021). Consumer personal data-driven digital marketing. *International Scientific Conference "New Challenges in Economic and Business Development – 2021: Post-Crisis Economy" proceedings*, *Latvia*, 150-159, https://www.bvef.lu.lv/fileadmin/user_upload/LU.LV/Apaksvietnes/Fakultates/www.bvef.lu.lv/Konferences/2021/Proceeding_of_Reports_2021.pdf.
20. EUI (2018). *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 LAW 2018/11, 1-90.
21. European Commission (2021). *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. https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52021pc0206
22. Unfair Commercial Practices Directive (2005). *European Parliament and Council Directive 2005/29/EC 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 L149/22.