14

Consumer Law as a Tool to Regulate Artificial Intelligence

Serge Gijrath

14.1 INTRODUCTION

Ongoing digital transformation combined with artificial intelligence (AI) brings serious advantages to society.[1] Transactional opportunities knock: optimal energy use, fully autonomous machines, electronic banking, medical analysis, constant access to digital platforms. Society at large is embracing the latest wave of AI applications as being one of the most transformative forces of our time. Two developments contribute to the rise of the algorithmic society: (1) the possibilities resulting from technological advances in machine learning, and (2) the availability of data analysis using algorithms. Where the aim is to promote competitive data markets, the question arises of what benefits or harm can be brought to private individuals. Some are concerned about human dignity.[2] They believe that human dignity may be threatened by digital traders who demonstrate an insatiable hunger for data.[3] Through algorithms the traders may predict, anticipate and regulate future private individual, specifically consumer, behaviour. Data assembly forms part of reciprocal transactions, where these data are currency. With the deployment of AI, traders can exclude uncertainty from the automated transaction processes.

The equality gap in the employment of technology to automated transactions begs the question of whether the private individual's fundamental rights are warranted adequately.[4] Prima facie, the consumer stands weak when she is subjected to automatic processes – no matter if it concerns day-to-day transactions, like boarding

[1] Press Release 19 February 2019, *Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence*.

[2] M. Tekmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, New York, 2017.

[3] For consistency purposes, this article refers to 'traders' when referring to suppliers and services providers. Art. 2(2) Directive 2011/83/EU *OJ L 304, 22 November 2011* (Consumer Rights Directive). See also Directive (EU) 2019/2161 amending Council Directive 93/13/EEC (Unfair Contract Terms Directive) and Directives 98/6/EC, 2005/29/EC and 2011/83/EU as regards the better enforcement and modernisation of Union consumer protection rules, *OJ L 328, 18 December 2019* (Modernization of Consumer Protection Directive).

[4] Council of Europe research shows that a large number of fundamental rights could be impacted from the use of AI, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

a train, or a complex decision tree used to validate a virtual mortgage. When 'computer says no' the consumer is left with limited options: click yes to transact (and, even then, she could fail), abort or restart the transaction process, or – much more difficult – obtain information or engage in renegotiations. But, where the negotiations process is almost fully automated and there is no human counterpart, the third option is circular rather than complementary to the first two. Empirical evidence suggests that automated decisions will be acceptable to humans only, if they are confident the used technology and the output is fair, trustworthy and corrigible.[5] How should Constitutional States respond to new technologies on multisided platforms that potentially shift the bargaining power to the traders?

A proposed definition of digital platforms is that these are companies (1) operating in two or multisided markets, where at least one side is open to the public; (2) whose services are accessed via the Internet (i.e., at a distance); and (3) that, as a consequence, enjoy particular types of powerful network effects.[6] With the use of AI, these platforms may create interdependence of demand between the different sides of the market. Interdependence may create indirect network externalities. This leads to establishing whether and, if so, how traders can deploy AI to attract one group of customers to attract the other, and to keep both groups thriving on the digital marketplace.

AI is a collection of technologies that combine data, algorithms and computing power. Yet science is unable to agree even on a single definition of the notion 'intelligence' as such. AI often is not defined either. Rather, its purpose is described. A starting point to understand algorithms is to see them as virtual agents. Agents learn, adapt and even deploy themselves in dynamic and uncertain virtual environments. Such learning is apt to create a static and reliable environment of automated transactions. AI *seems* to entail the replication of human behaviour, through data analysis that models 'some aspect of the world'. But does it? AI employs data analysis models to map behavioural aspects of humans.[7] Inferences from these models are used to predict and anticipate possible future events.[8] The difference in applying AI rather than standard methods of data analysis is that AI does *not* analyse data as they were programmed initially. Rather, AI assembles data, learns from them to respond

[5] B. Custers et al., *e-Sides, deliverable 2.2, Lists of Ethical, Legal, Societal and Economic Issues of Big Data Technologies. Ethical and Societal Implications of Data Sciences*, https://e-sides.eu/resources/deliverable-22-lists-of-ethical-legal-societal-and-economic-issues-of-big-data-technologies accessed 12 April 2019 (e-SIDES, 2017).

[6] H. Feld, *The Case for the Digital Platform Act: Breakups, Starfish Problems, & Tech Regulation*, e-book, 2019.

[7] UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making*, 2016. OECD, *Algorithms and Collusion – Background Note by the Secretariat*, DAF/COMP (2017) 4 (OECD 2017).

[8] The Society for the Study of Artificial Intelligence and Simulation of Behaviour, 'What Is Artificial Intelligence', *AISB Website* (no longer accessible); Government Office for Science, *Artificial Intelligence: Opportunities and Implications for the Future of Decision Making*, 9 November 2016; Information Commissioner's Office, UK, *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, Report, v. 2.2, 20170904 (ICO 2017).

intelligently to new data, and adapt the output in accordance therewith. Thus AI is not ideal for linear analysis of data in the manner they have been processed or programmed. Conversely, algorithms are more dynamic, since they apply machine learning.[9]

Machine learning algorithms build a *mathematical model* based on sample data, known as '*training data*'.[10] Training data serve computer systems to make predictions or decisions, without being programmed specifically to perform the task. Machine learning focuses on prediction-based unknown properties learned from the training data. Conversely, data analysis focuses on the discovery of (previously) unknown properties in the data. The analytics process enables the processor to mine data for new insights and to find correlations between apparently disparate data sets through self-learning. Self-learning AI can be supervised or unsupervised. Supervised learning is based on algorithms that build and rely on labelled data sets. The algorithms are 'trained' to map from input to output, by the provision of data with 'correct' values already assigned to them. The first training phase creates models on which predictions can then be made in the second 'prediction' phase.[11] Unsupervised learning entails that the algorithms are 'left to themselves' to find regularities in input data without any instructions on what to look for.[12] It is the ability of the algorithms to change their output based on experience that gives machine learning its power.

For humans, it is practically impossible to deduct and contest in an adequate manner the veracity of a machine learning process and the subsequent outcome based thereon. This chapter contends that the deployment of AI on digital platforms could lead to potentially harmful situations for consumers given the circularity of algorithms and data. Policy makers struggle with formulating answers. In Europe, the focus has been on establishing that AI systems should be transparent, traceable and guarantee human oversight.[13] These principles form the basis of this chapter. Traceability of AI could contribute to another requirement for AI in the algorithmic society: veracity, or truthfulness of data.[14] Veracity and truthfulness of data are subject to the self-learning AI output.[15] In accepting the veracity of the data, humans

[9] J. R. Koza, F. H. Bennett, D. Andre, and M. A. Keane 'Paraphrasing Arthur Samuel (1959), the Question Is: How Can Computers Learn to Solve Problems without Being Explicitly Programmed?' In *Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. Artificial Intelligence in Design*, Springer, 1996, 151–170. L. Bell, 'Machine Learning versus AI: What's the Difference?' *Wired*, 2 December 2016.

[10] C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer Verlag, 2006.

[11] ICO 2017, p. 7.

[12] E. Alpaydin, *Introduction to Machine Learning*, MIT Press, 2014.

[13] European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, 19 February 2019, COM(2020) 65 final.

[14] ' The quality of being true, honest, or accurate', *Cambridge Dictionary*, Cambridge University Press, 2020.

[15] J. Modrall, 'Big Data and Algorithms, Focusing the Discussion', Oxford University, *Business Law Blog*, 15 January 2018; D. Landau, 'Artificial Intelligence and Machine Learning: How Computers Learn', *iQ*, 17 August 2016, https://iq.intel.com/artificial-intelligence-and-machine-learning, now presented as 'A Data-Centric Portfolio for AI, Analytics and Cloud'; last accessed 14 March 2019.

require trust. Transparency is key to establishing trust. However, many algorithms are non-transparent and thus incapable of explanation to humans. Even if transparent algorithms would be capable of explanation to humans, then still the most effective machine learning process would defy human understanding. Hence the search for transparent algorithms is unlikely to provide insights into the underlying technology.[16] The quality of output using non-transparent AI is probably better, but it makes the position of the recipient worse, because there is no way for her to test the processes. Consequently, the Constitutional States may want to contain the potential harms of these technologies by applying private law principles.

This chapter's principal research question is how Constitutional States should deal with new forms of private power in the algorithmic society. In particular, the theorem is that regulatory private law can be revamped in the consumer rights' realm to serve as a tool to regulate AI and the possible adverse consequences for the weaker party on digital platforms. Rather than the top-down regulation of AI's consequences to protect human dignity, this chapter proposes considering a bottom-up approach of empowering consumers in the negotiations and the governance phases of mutual digital platform transactions. Following the main question, it must be seen how consumer rights can be applied to AI in a meaningful and effective manner. Could AI output be governed better if the trader must comply with certain consumer law principles such as contestability, traceability, veracity, and transparency?

One initial objection may query why we limit this chapter to consumer law. The answer is that consumers are affected directly when there is no room to negotiate or contest a transaction. Consumer rights are fundamental rights.[17] The Charter of Fundamental Rights of the EU (CFREU) dictates that the Union's policies 'shall ensure a high level of consumer protection'.[18] The high level of consumer protection is sustained by ensuring, inter alia, the consumers' economic interests in the Treaty on the Functioning of the European Union (TFEU).[19] The TFEU stipulates that the Union must promote consumers' rights to information. The TFEU stipulates that the Union must contribute to the attainment of a high-level baseline of consumer protection that also takes into account technological advances.[20] It is evident that in the algorithmic society, the EU will strive to control technologies if these potentially cause harm to the foundations of European private law. Responding adequately to the impact that AI deployment may have on private law norms and principles, a technology and private law approach to AI could,

[16] W. Seymour, 'Detecting Bias: Does an Algorithm Have to Be Transparent in Order to Be Fair?', www .CEUR-WS.org, vol. 2103 (2017).

[17] Art. 38 Charter of Fundamental Rights of the EU (CFREU).

[18] Art. 38 Fundamental Rights Charter.

[19] Article 169(1) and point (a) of Article 169(2) TFEU.

[20] Article 114 (3) of the Treaty on the Functioning of the European Union (TFEU). This clause mentions that within their respective powers, the European Parliament and the Council will also seek to achieve a high level of consumer protection.

conversely, enforce European private law.[21] Although AI is a global phenomenon, it is challenging to formulate a transnational law approach, given the lack of global AI and consumer regulation.

The structure is as follows: Section 14.2 sets the stage: AI on digital platforms is discussed bottom-up in the context of EU personal data and internal market regulation, in particular revamped consumer law, online intermediary[22] and free-flow of data regulation. The focus is on contributing to the ongoing governance debate of how to secure a high level of consumer protection when AI impacts consumer transactions on digital platforms, along with what rights consumers should have if they want to contest or reject AI output. Section 14.2.1 explores why consumer law must supplement AI regulation to warrant effective redress. Section 14.2.2 alludes to principles of contract law. Section 14.2.3 juxtaposes consumer rights with the data strategy objectives. Section 14.2.4 discusses trustworthiness and transparency. Section 14.3 is designed to align consumer rights with AI. Section 14.3.1 reflects on the regulation of AI and consumer rights through GTC. Section 14.3.2 presents consumer law principles that could be regulated: contestability (Section 14.3.2.1), traceability and veracity (Section 14.3.2.2) and transparency (Section 14.3.2.3). Section 14.3.3 considers further harmonization of consumer law in the context of AI. Section 14.4 contains closing remarks and some recommendations.

14.2 AI ON DIGITAL PLATFORMS

14.2.1 *Consumers, Data Subjects and Redress*

Consumers may think they are protected against adverse consequences of AI under privacy regulations and personal data protection regulatory regimes. However, it remains to be seen whether personal data protection extends to AI. Privacy policies are not designed to protect consumers against adverse consequences of data generated through AI. In that sense, there is a significant conceptual difference between policies and GTC: privacy policies are unilateral statements for compliance purposes. The policies do not leave room for negotiation. Moreover, privacy policies contain fairly moot purpose limitations. The purpose limitations are formulated de facto as processing rights. The private consumers/data subjects consider their

[21] Reiner Schulze, 'European Private Law: Political Foundations and Current Challenges' and J. M. Smits, 'Plurality of Sources in European Private Law', in R. Brownsword, H.-W. Micklitz, L. Niglia, and S. Weatherill, *The Foundations of European Private Law*, Oxford, 2011, p. 303–306 and 327*ff*.

[22] The Modernization of Consumer Protection Directive and Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services *OJ L 186*, 11 July 2019 (Online Intermediary Services Regulation). Regulation (EU) 2018/1807 of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, *OJ* L 303/59, 28 November 2018, entry into force May 2019 (Free Flow of Non-Personal Data Regulation).

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

consent implied to data processing, whatever tech is employed. Hence, the traders might be apt to apply their policies to consumers who are subjected to AI and machine learning. The General Data Protection Regulation (GDPR) contains one qualification in the realm of AI:[23] a data subject has the right *to object* at any time against ADM including profiling. This obligation for data controllers is set off by the provision that controllers may employ ADM, provided they demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

Most of the traders' machine learning is fed by aggregated, large batches of pseudonymised or anonymised non-personal data.[24] There is no built-in yes/no button to express consent to be subjected to AI, and there is no such regulation on the horizon.[25] The data policies are less tailored than GTC to defining consumer rights for complex AI systems. Besides, it is likely that most private individuals do not read the digital privacy policies – nor the general contract terms and conditions (GTC) for that matter – prior to responding to AI output.[26] The provided questions reveal important private law concerns: 'What are my rights?' relates to justified questions as regards access rights and vested consumer rights, the right to take note of and save/print the conditions; void unfair user terms; and termination rights. Traders usually refer to the GTC that can be found on the site. There is no meaningful choice. That is even more the case in the continental tradition, where acceptance of GTC is explicit. In Anglo-American jurisdictions, the private individual is confronted with a pop-up window which must be scrolled through and accepted. Declining means aborting the transaction.

'How can I enforce my rights against the trader?' requires that the consumer who wishes to enforce her rights must be able to address the trader, either on the platform or through online dispute resolution mechanisms. Voidance or nullification are remedies when an agreement came about through settled European private law principles, such as coercion, error or deceit. Hence the consumer needs to know there is a remedy if the AI process contained errors or was faulty.[27]

[23] Council Regulation (EU) 2016/679 on the on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ L* 119/1 (General Data Protection Regulation, or GDPR) contains the right to object and automated individual decision-making (articles 21–22 GDPR), subject to fairly complex exclusions that are explained in detail in the extensive considerations.

[24] There is no legal basis under when there are no personal data involved; section 3, e.g., articles 16 (rectification), 17 (erasure), 18 (restriction on processing), and 20 (data portability) GDPR – the rights are often qualified, and the burden of proof is not clear. This makes the consumer's rights rather difficult to enforce.

[25] H. U. Vrabec, *Uncontrollable Data Subject Rights and the Data-Driven Economy*, dissertation, University Leiden, 2019.

[26] See *Eurobarometer Special 447 on Online Platforms* (2016).

[27] This chapter does not discuss online dispute resolution.

14.2.2 *Principles of Contract Law*

In the algorithmic society, consumers still should have at least some recourse to a counterparty, whom they can ask for information during the consideration process. They must have redress when they do not understand or agree with transactional output that affects their contractual position without explanation. The right to correct steps in contract formation is moot, where the process is cast in stone. Once the consumers have succeeded in identifying the formal counterparty, they can apply remedies. Where does that leave them if the response to these remedies is also automated as a result of the trader's use of profiling and decision-making tools? This reiterates the question of whether human dignity is at stake, when the counterpart is not a human but a machine. The consumer becomes a string of codes and loses her feeling of uniqueness.[28] Furthermore, when distributed ledger technology is used, the chain of contracts is extended. There is the possibility that an earlier contractual link will be 'lost'. For example, there is a gap in the formation on the digital platform, because the contract formation requirements either were not fully met or were waived. Another example is where the consumer wants to partially rescind the transaction but the system does not cater for a partial breach. The impact of a broken upstream contractual link on a downstream contract in an AI-enabled transactional system is likely to raise novel contract law questions, too. An agreement may lack contractual force if there is uncertainty or if a downstream contractual link in the chain is dependent on the performance of anterior upstream agreements. An almost limitless range of possibilities will need to be addressed in software terms, in order to execute the platform transaction validly. When the formation steps are using automated decision-making processes that are not covered in the GTC governing the status of AI output, then this begs the question of how AI using distributed ledger technology could react to non-standard events or conditions, and if and how the chain of transactions is part of the consideration. The consumer could wind up in a vicious cycle, and her fundamental rights of a high consumer protection level could be at stake, more than was the case in the information society. Whereas e-Commerce, Distant Selling and, later, Services Directives imposed information duties on traders, the normative framework for the algorithmic society is based on rather different principles. Theories such as freedom of contract – which entails the exclusion of coercion – and error, when AI output contains flaws or defects may be unenforceable in practice. For the consumer to invoke lack of will theories, she needs to be able to establish where and how in the system the flaws or mistakes occurred.

[28] Spike Jonze, *Her* (2013). In this movie, the protagonist in an algorithmic society develops an intimate relationship with his operating system – that is, until he finds out the operating system communicates with millions of customers simultaneously.

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

14.2.3 Data Strategy

Does the data strategy stand in the way of consumer protection against AI? The focus of the EU's data strategy is on stimulating the potential of data for business, research and innovation purposes.[29] The old regulatory dilemma on how to balance a fair and competitive business environment with a high level of consumer rights is revived. In 2019–2020, the Commission announced various initiatives, including rules on (1) securing free flow of data within the Union,[30] (2) provisions on data access and transfer,[31] and (3) and enhanced data portability.[32] Prima facie, these topics exhibit different approaches to achieve a balance between business and consumer interests. More importantly, how does the political desire for trustworthy technology match with such diverse regulations? The answer is that it does not. The Free Flow of Non-Personal Data Regulation lays down data localization requirements, the availability of data to competent authorities and data porting for professional users.[33] It does not cover AI use. The Modernization of Consumer Protection Directive alludes to the requirement for traders to inform consumers about the default main parameters determining the ranking of offers presented to the consumer as a result of the search query and their relative importance as opposed to other parameters only.[34] The proviso contains a reference to 'processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the ranking are not required to disclose the detailed functioning of their ranking mechanisms, including algorithms'.[35] It does not appear that the Modernization of Consumer Protection Directive is going to protect consumers against adverse consequences of AI output. It also seems that the Trade Secrets Directive stands somewhat in the way of algorithmic transparency.

The provisions on data porting revert to information duties. Codes of Conduct must detail the information on data porting conditions (including technical and operational requirements) that traders should make available to their private individuals in a sufficiently detailed, clear and transparent manner before a contract is

[29] Directive (EU) 2019/1024 on open data and the re-use of public sector information, *OJ* L 172/56 (Open Data Directive); *Commission Communication*, 'Building a European Data Economy', COM (2017) 9 final.

[30] Free Flow of Non-Personal Data Regulation.

[31] Regulation 2017/1128/EU of the European Parliament and of the Council of 14 June 2017 on Cross-border Portability of Online Content Services in the Internal Market, [2017] *OJ* L 168/1 including corrigendum to regulation 2017/1128.

[32] GDPR, articles 13 and 20.

[33] The Free Flow of Non-Personal Data Regulation does not define 'non-personal data'. Cf. art. 3 of the Non-personal Data Regulation: '"Data" means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679'.

[34] Modernization of Consumer Protection Directive, recital (22).

[35] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure *OJ* L 157 (Trade Secrets Directive).

concluded.[36] In light of the limited scope of data portability regulation, there can be some doubt as to whether the high-level European data strategy is going to contribute to a human-centric development of AI.

14.2.4 Trustworthiness and Transparency

The next question is what regulatory requirements could emerge when AI will become ubiquitous in mutual transactions.[37] The Ethical Guidelines on AI in 2019 allude to seven key requirements for 'Trustworthy AI': (1) human agency and oversight; (2) technical robustness and safety; (3) privacy and data governance; (4) transparency, (5) diversity, non-discrimination and fairness; (6) environmental and societal well-being; and (7) accountability.[38] These non-binding guidelines address different topics, some of which fall outside the scope of private law principles. In this chapter, the focus is on transparency, accountability and other norms, notably traceability, contestability and veracity.[39] These notions are covered in the following discussion. First, it is established that opaqueness on technology use and lack of accountability could be perceived as being potentially harmful to consumers.[40] There are voices that claim that technology trustworthiness is essential for citizens and businesses that interact.[41] Is it up to Constitutional States to warrant and monitor technology trustworthiness, or should this be left to businesses? Does warranting technology trustworthiness not revive complex economic questions, such as how to deal with the possibility of adverse impact on competition or the stifling of innovation, when governments impose standardized technology norms to achieve a common level of technology trustworthiness – in the EU only? What if trust in AI is broken?

A possible denominator for trustworthiness may be transparency. Transparency is a key principle in different areas of EU law. A brief exploration of existing regulation reveals different tools to regulate transparency. Recent examples in 2019–2020 range from the Modernization of Consumer Protection Directive to the Online

[36] Commission Communication DSM 2017, p. 2. The Commission mentions a number of activities, including online advertising platforms, marketplaces, search engines, social media and creative content outlets, application distribution platforms, communications services, payment systems and collaboration platforms.

[37] *Commission Communication on Shaping Europe's Digital Future*, Brussels, 19.2.2020 COM (2020) 67 final; *White Chapter on Artificial Intelligence*, setting out options for a legislative framework for trustworthy AI, with a follow-up on safety, liability, fundamental rights and data (Commission Communication 2020).

[38] Following two *Commission Communications* on AI supporting 'ethical, secure and cutting-edge AI made in Europe' (COM (2018)237 and COM (2018)795), a High-Level Expert Group on Artificial Intelligence was established: *Ethic Guidelines for Trustworthy AI*, 8 April 2019 (COM (2019)168; Ethic Guidelines AI 2019); https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. The Guidelines seem to have been overridden by the White Paper AI 2020.

[39] Ethic Guidelines AI 2019, p. 2.

[40] e-Sides 2017, i.a., p. 85*ff.*, and the attached lists.

[41] Commission Communication AI 2018, para. 3.3.

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

Intermediary Services Regulation, the Ethical Guidelines on AI, the Open Data Directive and the 2020 White Paper on Artificial Intelligence.[42] All these instruments at least allude to the need for transparency in the algorithmic society. The Modernization of Consumer Protection Directive provides that more transparency requirements should be introduced. Would it be necessary to redefine transparency as a principle of private law in the algorithmic society? One could take this a step further: to achieve technology trustworthiness, should there be more focus on regulating *transparency* of AI and machine learning?[43] The Ethics Guidelines 2019 point at permission systems, fairness and explicability. From a private law perspective, especially permission systems could be considered to establish and safeguard trust. But reference is also made to the factual problem that consumers often do not take note of the provisions that drive the permission.

Explicability is not enshrined as a guiding principle. Nevertheless, transparency notions could be a stepping stone to obtaining explicability.[44] Accuracy may be a given. What matters is whether the consumer has the right and is enabled to contest an outcome that is presented as accurate.

14.3 CONSUMER RIGHTS, AI AND ADM

14.3.1 *Regulating AI through General Terms and Conditions*

There are two aspects regarding GTC that must be considered. First, contrary to permission systems, the general rule in private law remains that explicit acceptance of GTC by the consumer is not required, as long as the trader has made the terms available prior to or at the moment the contract is concluded. Contrary to jurisdictions that require parties to scroll through the terms, the European approach of accepting implied acceptance in practice leads to consumers' passiveness. Indeed, the system of implicit permission encourages consumers to not read GTC. Traders on digital platforms need to provide information on what technologies they use and how they are applied. Given the sheer importance of fundamental rights of human dignity and consumer rights when AI is applied, the question is whether consumers should be asked for explicit consent when the trader applies AI. It would be very simple for traders to implement consent buttons applying varied decision trees. But what is the use when humans must click through to complete a transaction? Take, for example, the system for obtaining cookies consent on digital platforms.[45] On the

[42] White Paper AI 2020.

[43] Ethic Guidelines AI 2019, p. 12–13: The Guidelines do not focus on consumers. Rather, the Guidelines address different stakeholders going in different directions.

[44] P. Beddington, *Towards a Code of Ethics for Artificial Intelligence*, Springer International Publishing, 2017.

[45] At the time of writing, the draft proposal Council Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC COM 2017 final (draft Regulation on Privacy and Electronic Communications) was in limbo.

one hand, the traders (must) provide transparency on which technologies they employ. On the other hand, cookie walls prevent the consumer from making an informed decision, as they are coerced to accept the cookies. A recognizable issue with cookies in comparison with AI is that, often, it is the consumers who are unable to understand what the different technologies could mean for them personally. In the event the AI output matches their expectations or requirements, consumers are unlikely to protest prior consent given. Hence the real question is whether consumers should be offered a menu of choice beforehand, plus an option to accept or reject AI output or ADM. This example will be covered in the following discussion.

Second, where there is no negotiation or modification of the GTC, the consumer still will be protected by her right to either void or rescind black-, blue or grey-list contract provisions. Additionally, the EU Unfair Contract Terms Directive contains a blue list with voidable terms and conditions.[46] However, the black, grey and blue lists do not count for much. Rather, the GTC should contain clauses that oblige the trader to observe norms and principles such as traceability, contestability, transparency and veracity of the AI process. This begs the question of whether ethics guidelines and new principles could be translated into binding, positively formulated obligations or AI use. Rather than unilateral statements on data use, GTC could be subjected to comply with general principles and obligations.

The key for prospective regulation does not lie in art. 6 (1) Modernization of Consumer Protection Directive. Although this clause contains no less than twenty-one provisions on information requirements, including two new requirements on technical aspects, none of the requirements apply to providing the consumer information on the use of AI and ADM, let alone the contestability of the consumer transaction based thereon. Granted, there is an obligation for the trader to provide information on the scope of the services, but not on the specific use of AI technology. It is a very big step from the general information requirements to providing specific information on the application of AI and ADM in mutual transactions. When a consumer is subjected to AI processes, she should be advised in advance, not informed after the fact. A commentary to art. 6 clarifies that the traders must provide the information mentioned therein *prior* to the consumer accepting the contract terms (GTC).[47] The underlying thought is not new – to protect consumers, as weaker contractual parties, from concluding contracts that may be detrimental to them, and as a result of not having all the necessary information. Absent any relevant information, the consumer lags behind, especially in terms of not being informed adequately (1) that, (2) how and (3) for which purposes AI and machine learning is applied by the trader. The commentators generally feel that providing consumers with the relevant information prior to the conclusion of the contract is essential.

[46] *Unfair Contract Terms Directive*.

[47] J. Luzak and S. van der Hof, part II, chapter 2, in *Concise European Data Protection, E-Commerce and IT Law*, S. J. H. Gijrath, S. van der Hof, A. R. Lodder, G.-J. Zwenne, eds., 3rd edition, Kluwer Law International, 2018.

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

Knowing that the trader uses such technologies could be of utmost importance to the consumer. Even if she cannot oversee what the technological possibilities are, she should still get advance notice of the application of AI. Advance notice means a stand-still period during which she can make an informed decision. Going back to the cookie policy example, it is not onerous on the trader to offer the consumer a menu for choice beforehand. This would be especially relevant for the most used application of AI and ADM: profiling. The consumer should have the right to reject a profile scan that contains parameters she does not find relevant or which she perceives as being onerous on her. Granted, the trader will warn the consumer that she will not benefit from the best outcome, but that should be her decision. The consumer should have a say in this important and unpredictable process. She should be entitled to anticipating adverse consequences of AI for her.

The consumer must be able to trace and contest the AI output and ADM. The justification for such rights is discrimination, and lack of information on the essentials underlying the contract terms that come about through the private law principle of offer and acceptance. Granted, art. 9 Modernization of Consumer Protection Directive contains the generic right of withdrawal.[48] Contesting a consumer transaction based on AI is not necessary. The consumer can simply fill in a form to rescind the agreement. Regardless, the point of a consumer approach to AI use is not meant for the consumer to walk away. The consumer must have the right to know what procedures were used, what kind of outcome they produced, what is meant for the transaction and what she can do against it. As said, the consumer also must have a form of redress, not just against the trader but also against the developer of the AI software, the creator of the process, the third-party instructing the algorithms and/or the intermediary or supplier of the trader.

14.3.2 *Consumer Law Principles*

Which consumer law principles could be reignited in GTC that enable consumers to require the traders to be accountable for unfair processes or non-transparent output? This goes back to the main theorem. Transactions on digital platforms are governed by mutually agreed contract terms. It is still common practice that these are contained in GTC. Is there a regulatory gap that requires for Constitutional States to formulate new or bend existing conditions for traders using AI? The Bureau Européen des Unions de Consommateurs[49] proposes 'a set of transparency obligations to make sure consumers are informed when using AI-based products and services, particularly about the functioning of the algorithms involved and rights to object automated decisions'. The Modernization of Consumer Protection Directive is open for adjustment of consumer rights 'in the context of continuous

[48] Cf. the standard withdrawal form in Annex 1 to the Consumer Rights Directive.

[49] Bureau Européen des Unions de Consommateurs AISBL, *Automated Decision Making and Artificial Intelligence – A Consumer Perspective*, Position Chapter 20 June 2018 (BEUC 2018).

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

development of digital tools'. The Directive makes a clear-cut case for consumers catering for the adverse consequences of AI.[50] But it contains little concrete wording on AI use and consumers.[51] Embedding legal obligations for the trader in GTC could, potentially, be a very effective measure. There is one caveat, in that GTC often contain negatively formulated obligations.[52] Positively phrased obligations, such as the obligation to inform consumers that the trader employs AI, require further conceptual thinking. Another positively phrased obligation could be for the traders to explain the AI process and explain and justify the AI output.

14.3.2.1 Contestability

How unfair is it when consumers may be subject to decisions that are cast in stone (i.e., non-contestable)? An example is embedded contestability steps in smart consumer contracts. At their core, smart contracts are self-executing arrangements that the computer can make, verify, execute and enforce automatically under event-driven conditions set in advance. From an AI perspective, an almost limitless range of possibilities must be addressed in software terms. It is unlikely that these possibilities can be revealed step-by-step to the consumer. Consumers probably are unaware of the means of redress against AI output used in consumer transactions.[53] Applying a notion of contestability – not against the transaction but against the applied profiling methods or AI output – is no fad. If the system enables the consumer to test the correctness of the AI technology process and output, there must be a possibility of reconsidering the scope of the transaction. Otherwise, the sole remedy for the consumer could be a re-test of the AI process, which is a fake resolve. Indeed, the possibility of technological error or fraud underlines that a re-test is not enough. Traditional contract law remedies, such as termination for cause, could be explored. Furthermore, in connection with the information requirements, it would make sense to oblige traders to grant the consumer a single point of contact. This facilitates contesting the outcome with the trader or a third party, even if the automated processes are not monitored by the trader.[54]

14.3.2.2 Traceability, Veracity

Testing veracity requires reproducibility of the non-transparent machine learning process. Does a consumer have a justified interest in tracing the process steps of

[50] Modernization of Consumer Protection Directive, recital (17).

[51] Cf. Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No. 2006/2004 (OJ L 345, 27.12.2017, p. 1).

[52] Cf. the Unfair Consumer Contract Terms Directive.

[53] Modernization of Consumer Protection Directive, consideration (2).

[54] Cf. the Online Intermediary Services Regulation where corrections can be made at the wholesale level.

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

machine learning, whether or not this has led to undesirable AI output? Something tells a lawyer that – no matter the output – as long as the AI output has an adverse impact on the consumer, it seems reasonable that the trader will have the burden of evidence that output is correct and, that, in order to be able to provide a meaningful correction request, the consumer should be provided with a minimum of necessary technical information that was used in the AI process. Traceability is closely connected with the requirement of accessibility to information, enshrined in the various legal instruments for digital platform regulation. As such, traceability is closely tied with the transparency norm.

It is likely that a trader using AI in a consumer transaction will escape from the onus on proving that the machine learning process, the AI output or the ADM is faulty. For the average consumer, it will be very difficult to provide evidence against the veracity of – both non-transparent *and* transparent – AI. The consumer is not the AI expert. The process of data analysis and machine learning does not rest in her hands. Besides, the trail of algorithmic decision steps probably is impossible to reconstruct. Hence, the consumer starts from a weaker position than the trader who applies AI. Granted, it was mentioned in Section 14.2.2 that it makes no practical sense for the consumer to ask for algorithmic transparency, should the consumer not agree with the output. The point is that at least the consumer should be given a chance to trace the process. Traceability – with the help of a third party who is able to audit the software trail – should be a requirement on the trader and a fundamental right for the consumer.

14.3.2.3 Transparency

Transparency is intended to solve information asymmetries with the consumer in the AI process. Transparency is tied closely with the information requirements laid down in the digital platforms and dating back to the Electronic Commerce Directive.[55] What is the consequence when information requirements are delisted because they have become technologically obsolete? Advocate General Pitruzzella proposed that the Court rule that an e-commerce platform such as Amazon could no longer be obliged to make a fax line available to consumers.[56] He also suggested that digital platforms must guarantee the choice of several different means of communication available for consumers and rapid contact

[55] 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 [2000] OJ L 178/1 (Electronic Commerce Directive).

[56] Modernization of Consumer Protection Directive, recital (46); CJEU ECLI:EU:C:2019:576, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Amazon EU Sàrl, request for a preliminary ruling from the Bundesgerichtshof, 10 July 2019. The Court followed the non-binding opinion of the Advocate-General to revoke trader's obligations to provide certain additional information, such as a telephone or fax number.

and efficient communication.[57] By analogy, in the algorithmic society, transparency obligations on AI-driven platforms could prove to be a palpable solution for consumers. Providing transparency on the output also contributes to the consumer exercising some control over data use in the AI process, notwithstanding the argument that transparent algorithms cannot be explained to a private individual.

14.3.3 *Further Harmonization of Consumer Law in the Context of AI*

It should be considered whether the Unfair Commercial Practices Directive could be updated with terms that regulate AI.[58] At the high level, this Directive introduced the notion of 'good faith' to prevent imbalances in the rights and obligations of consumers on the one hand and sellers and suppliers on the other hand.[59] It should be borne in mind that consumer protection will become an even more important factor when the chain of consumer agreements with a trader becomes extended. Granted, the question of whether and how to apply AI requires further thinking on what types of AI and data use could constitute unfair contract terms. A case could be made of an earlier agreement voiding follow-up transactions, for example, because the initial contract formation requirements were not met as after AI deployment. But the impact of a voidable upstream contractual link on a downstream agreement in an AI-enabled or contract system is likely to raise different novel contract law questions, for instance, regarding third party liability.

In order to ensure that Member State authorities can impose effective, proportionate and dissuasive penalties in relation to widespread infringements of consumer law and to widespread infringements with an EU dimension that are subject to coordinated investigation and enforcement,[60] special fines could be introduced for the unfair application of AI.[61] Contractual remedies, including claims as a result of damages suffered from incorrect ADM, could be considered.

Prima facie, the Modernization of Consumer Protection Directive provides for the inclusion of transparency norms related to the parameters of ranking of prices and persons on digital platforms. However, the Directive does not contain an obligation to inform the consumer about the relative importance of ranking parameters and the reasons why and through what human process, if any, the input criteria were determined. This approach bodes well for the data strategy, but consumers

[57] Advocate General's Opinion in Case C-649/17 *Bundesverband der Verbraucherzentralen and Others* v. *Amazon EU*, CJEU, Press Release No. 22/19 Luxembourg, 28 February 2019.

[58] 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 (Unfair Commercial Practices Directive 2005), *OJ* 2005, L. 149.

[59] Unfair Contract Terms Directive, p. 29–34.

[60] Regulation (EU) 2017/2394.

[61] In order to ensure deterrence of the fines, Member States should set in their national law the maximum fine for such infringements at a level that is at least 4 per cent of the trader's annual turnover in the Member State or Member States concerned. Traders in certain cases can also be groups of companies.

could end up unhappy, for instance, if information about the underlying algorithms is not included in the transparency standard.

By way of an example, the Modernization of Consumer Protection Directive provides for a modest price transparency obligation at the retail level. It proposes a specific information requirement to inform consumers clearly when the price of a product or service presented to them is personalized on the basis of ADM. The purpose of this clause is to ensure that consumers can take into account the potential price risks in their purchasing decision.[62] But the proviso does not go as far as to determine how the consumer should identify these risks. Digital platforms are notoriously silent on price comparisons. Lacking guidance on risk identification results in a limited practical application of pricing transparency. What does not really help is that the Modernization of Consumer Protection Directive provides traders with a legal – if flimsy – basis for profiling and ADM.[63] This legal basis is, unfortunately, not supplemented by consumer rights that go beyond them receiving certain, non-specific information from the trader. The Modernization of Consumer Protection Directive, as it stands now, does not pass the test of a satisfactorily high threshold for consumer protection on AI-driven platforms.

14.4 CLOSING REMARKS

This chapter makes a case for a bottom-up approach to AI use in consumer transactions. The theorem was that the use of AI could well clash with the fundamental right of a high level of consumer protection. Looking at principles of contract law, there could be a regulatory gap when traders fail to be transparent on why and how they employ AI. Consumers also require a better understanding of AI processes and consequences of output, and should be allowed to contest the AI output.

Regulators alike could look at enhancing GTC provisions, to the extent that the individual does not bear the onus of evidence when contesting AI output. Consumers should have the right to ask for correction, modification and deletion of output directly from the traders. It should be borne in mind that the individual is contesting the way the output was produced, generated and used. The argument was made also that consumer rights could supplement the very limited personal data rights on AI.

When Constitutional States determine what requirements could be included in GTC by the trader, they could consider a list of the transparency principles. The list could include (1) informing the consumer prior to any contract being entered into that it is using AI; (2) clarifying for what purposes AI is used; (3) providing the consumer with information on the technology used; (4) granting the consumer

[62] 'Pricing that involves changing the price in a highly flexible and quick manner in response to market demands when it does not involve personalisation based on automated decision making.' Directive 2011/83/EU.

[63] Modernization of Consumer Protection Directive, recital (45).

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press

a meaningful, tailored and easy to use number of options in accepting or rejecting the use of AI and/or ADM, before it engages in such practice; (5) informing the consumer beforehand of possible adverse consequences for her if she refuses to submit to the AI; (6) how to require from the trader a rerun on contested AI output; (7) adhering to an industry-approved code of conduct on AI and making this code easily accessible for the consumer; (8) informing the consumer that online dispute resolution extends to contesting AI output and/or ADM; (9) informing the consumer that her rights under the GTC are without prejudice to other rights such under personal data regulation; (10) enabling the consumer – with one or more buttons – to say yes or no to any AI output, and giving her alternative choices; (11) enabling the consumer to contest the AI output or ADM outcome; (12) accepting liability for incorrect, discriminatory and wrongful output; (13) warranting the traceability of the technological processes used and allowing for an audit at reasonable cost and (14) explaining the obligations related to how consumer contracts are shared with a third party performing the AI process. These suggestions require being entitled to have a human, independent third party to monitor AI output, and the onus of evidence regarding the veracity of the output should be on the trader.

The fact that AI is aimed at casting algorithmic processes in stone to facilitate mutual transactions on digital platforms should not give traders a carte blanche, when society perceives a regulatory gap.

https://doi.org/10.1017/9781108914857.015 Published online by Cambridge University Press