



*Emanuele Scattarreggia\**

## GENERAL SECTION

# AI-DRIVEN SMART CONTRACTS

## ENHANCING CONSUMER PROTECTION OR EXACERBATING CONSUMER PROTECTION CHALLENGES?

### *Abstract*

The integration of artificial intelligence (AI) into smart contracts holds the potential to both enhance and exacerbate consumer protection challenges. Since the AI system embedded within the contract's code enables a high degree of contractual personalisation - by tailoring the legal agreement to the unique characteristics of the targeted individual consumer, thanks to its capacity to process large amounts of personal and behavioural data in real time - it opens the door not only to scenarios of AI-powered consumer manipulation, but also to the promising opportunity of a consumer-centric AI. Such an AI would serve the consumer's best interests by adapting the contract to their specific needs and preferences, while protecting them from - rather than exploiting - their information, cognitive, and digital vulnerabilities. This research aims to assess whether the EU legal framework - particularly the UCPD, UCTD, AI Act, GDPR, and DSA - adequately ensures that these technologies are designed and deployed with the consumer's well-being at their core. The paper explores AI-related risks such as digital manipulation, personal data exploitation, and the black-box problem inherent in algorithmic opacity, while also addressing the liability challenge in cases of consumer harm. Ultimately, it seeks to answer whether AI-driven smart contracts can truly foster a high level of consumer protection in the AI era, by offering novel interpretations of the existing legal framework and advancing proposals for reform aligned with the fairness-by-design approach and informed by behavioural science insights.

**JEL CLASSIFICATION:** K11, K12, K13, K15, K24, K38, K42

### SUMMARY

1 Introduction - 2 AI-Driven Smart Contracts & Manipulation Risks - 2.1 The Role of the UCPD and the UCTD - 2.2 The Role of the AI Act - 2.3 Algorithmic Vulnerability - 3 AI-Driven Smart Contracts & GDPR Compliance - 3.1 The Privacy-By-Design Solution - 3.2 Automated Decision-Making - 3.3 A Legal Crossroads - 4 AI-Driven Smart Contracts & the DSA - 4.1 Platform Liability - 4.2 The Content Moderation Challenge - 4.3 Algorithmic

---

\* PhD student in Law at the University of Sydney. E-mail: [esca0791@uni.sydney.edu.au](mailto:esca0791@uni.sydney.edu.au).

Accountability & Transparency Obligation - 5 Liability: Centralised vs. Decentralised Platforms - 6 AI-Driven Smart Contracts Transparency - 6.1 The Black-Box Problem & a Possible Solution - 6.2 The Need for Human Oversight & Intervention - 7 A Possible Way Forward: The Fairness-by-Design Approach - 8 Conclusion

## 1 Introduction

The integration of artificial intelligence (AI) into smart contracts marks a significant shift in digital legal agreements, with the potential to both enhance and complicate consumer protection<sup>1</sup> within the European Union (EU). Smart contracts - self-executing agreements based on predefined rules (*if* a condition is met, *then* the obligation is performed) - have long been praised for their efficiency<sup>2</sup>, automation<sup>3</sup>, and ability to reduce transaction costs<sup>4</sup>. However, these advantages also introduce legal and ethical challenges, particularly in consumer protection<sup>5</sup>. The EU has sought to safeguard consumers through legal acts - such as the Unfair Commercial Practices Directive (UCPD<sup>6</sup>), Unfair Contract Terms Directive (UCTD<sup>7</sup>), General Data Protection Regulation (GDPR<sup>8</sup>), AI Act<sup>9</sup>, and Digital Services Act (DSA<sup>10</sup>). Yet, as AI-driven smart contracts evolve, they present new complexities that existing legal frameworks struggle to address, highlighting the pressing need for future-proof regulation.

AI-driven smart contracts bring greater adaptability and compliance monitoring, potentially improving fairness and transparency by dynamically adjusting contract terms and predicting legal risks. AI can automate compliance with EU (and domestic) laws, ensuring contracts respect consumer rights, privacy, and non-discrimination principles. However, these contracts also introduce new risks, including opacity in decision-making (black-box AI), potential biases, and challenges in accountability and liability.

This paper examines whether AI-driven smart contracts ultimately enhance consumer protection or exacerbate regulatory challenges, by addressing the following overarching research question:

- Can AI-driven smart contracts ensure a high level of consumer protection in the EU?

---

<sup>1</sup> See Pinar C Aksoy, 'AI and Smart Consumer Contracts' in Larry A DiMatteo and others (eds), *The Cambridge Handbook of AI and Consumer Law* (Cambridge University Press 2024) 99-115.

<sup>2</sup> Ohm Patel, 'AI-Driven Smart Contracts' (2024) 3(4) *Journal of Artificial Intelligence & Cloud Computing* 1-4.

<sup>3</sup> Alexander Savelyev, 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law' (2016) Higher School of Economics Research Paper No. WP BRP 71/LAW/2016 <<https://ssrn.com/abstract=2885241>> accessed 28 May 2025.

<sup>4</sup> See Lin W Cong and others, 'Scaling Smart Contracts via Layer-2 Technologies: Some Empirical Evidence' (2023) 69 (12) *Management Science* 7306-7316. Cf. Massimiliano Vatiery, 'Smart contracts and transaction costs' (*Oxford Law Blogs*, 10 October 2018) <<https://blogs.law.ox.ac.uk/business-law-blog/blog/2018/10/smart-contracts-and-transaction-costs>> accessed 28 May 2025.

<sup>5</sup> See Geraint Howells, 'Protecting Consumer Protection Values in the Fourth Industrial Revolution' (2020) 43 *Journal of Consumer Policy* 154-158.

<sup>6</sup> Directive 2005/29/EC.

<sup>7</sup> Council Directive 93/13/EEC.

<sup>8</sup> Regulation (EU) 2016/679.

<sup>9</sup> Regulation (EU) 2024/1689.

<sup>10</sup> Regulation (EU) 2022/2065.



To answer this question, it explores manipulative AI practices, privacy risks, transparency concerns, and the need for regulatory adaptation, drawing on interdisciplinary insights from law, economics, and behavioural science. Finally, this paper proposes a fairness-by-design approach as a possible regulatory solution to ensure that AI-driven smart contracts align with EU consumer protection goals.

## 2 AI-Driven Smart Contracts & Manipulation Risks

The integration of AI into smart contracts<sup>11</sup> introduces novel consumer protection concerns, particularly in relation to manipulative practices that rely on algorithmic, data-driven analyses to tailor contract terms to the individual consumer they address<sup>12</sup>. Unlike traditional smart contracts, which operate on predefined and unmodifiable rules without adaptability, AI-driven smart contracts can dynamically modify contract terms and conditions based on real-time data<sup>13</sup>. By analysing and profiling consumers, including their online behaviour<sup>14</sup>, they enable a high degree of contractual personalisation. While this adaptability can enhance efficiency and fairness - especially when these flexible features are used to better protect consumers from their information, cognitive, and digital vulnerabilities - it also has the potential to create new asymmetries of power between traders and consumers<sup>15</sup>.

One of the most pressing concerns is *digital manipulation*<sup>16</sup>. AI-driven smart contracts can leverage machine learning to detect patterns in consumer behaviour, preferences, and decision-making processes, allowing firms to optimise contract terms in ways that

---

<sup>11</sup> See Gérardine Goh Escolar, 'Addressing Digital Vulnerability Through Private International Law' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos 2024) 344.

<sup>12</sup> AI's ability to process data and personalise outputs for its individual recipient may further expose the vulnerability condition, which is an intrinsic characteristic of all human beings. This could lead to a shift in consumer protection standards, where the vulnerable consumer becomes the norm rather than the exception, challenging the traditional average consumer standard. Cf. Geraint Howells (n 1) 5. On vulnerability as a universal human condition, see e.g. Martha A Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20 *Yale Journal of Law & Feminism* 1, 1-23.

<sup>13</sup> On the adaptability potential of smart contracts interacting with real-time data, see e.g. Oluwafemi Elias and others, 'The evolution of green fintech: Leveraging AI and IoT for sustainable financial services and smart contracts implementation' (2024) 23 *World Journal of Advanced Research and Reviews* 1, 2717. See also OECD, 'Artificial Intelligence, Machine Learning and Big Data in Finance. Opportunities, Challenges, and Implications for Policy Makers' (2021) <[https://www.oecd.org/en/publications/artificial-intelligence-machine-learning-and-big-data-in-finance\\_98e761e7-en.html](https://www.oecd.org/en/publications/artificial-intelligence-machine-learning-and-big-data-in-finance_98e761e7-en.html)> accessed 28 May 2025, 34-35.

<sup>14</sup> The technique is similar to that employed by recommender systems: the AI system analyses consumer data to deliver a personalised output - namely, contract clauses. Moreover, the visual representation of the legal agreement and the way information is highlighted may be tailored to the specific consumer targeted by the trader. Given this, the effectiveness of the output in terms of the consumer's well-being depends on two key factors: 1) the quality of the data processed and the efficiency of the processing system; and 2) the good intentions of the traders, who must prioritise consumer interests over merely maximising corporate profits. Cf. Luigi Portinale and Alessandro Abuton, 'Artificial Intelligence for Consumers. Advances in Recommendation Systems' in Larry A DiMatteo and others (eds) (n 1) 9-18. See also Hal R Varian, 'Computer Mediated Transactions' (2010) 100 *The American Economic Review* 2, 6.

<sup>15</sup> Cf. Mateja Durovic, 'AI and Existing EU Consumer Law' in Larry A. DiMatteo and others (eds) (n 1) 49-50.

<sup>16</sup> i.e., behavioural manipulation in a digital environment. It involves the use of digital technologies to exploit consumer emotional and cognitive vulnerabilities. See Philipp Hacker, 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection and privacy law' (2023) 29 *Eur Law J.* 142-175.

benefit traders at the expense of consumers<sup>17</sup>. For example, AI could enable more sophisticated trader strategies of personalised pricing, adjust fees based on an individual's willingness to pay, or introduce exploitative terms tailored to specific consumer vulnerabilities<sup>18</sup>. Moreover, the use of *dark patterns*<sup>19</sup> - user interface designs that nudge users into making decisions they would not have otherwise made, to the detriment of their well-being - becomes particularly problematic, when incorporated into AI-driven smart contracts, as AI personalises these tactics through psychological profiling.

Finally, it is crucial to underscore that efficient markets rely on consumers making efficient choices. If AI-driven manipulation distorts the consumer decision-making process, competition risks devolving into a scenario where *the best manipulator wins*. Preventing such risks is essential to ensuring a healthy digital single market.

## 2.1 The role of the UCPD and the UCTD

Framing effects<sup>20</sup> and persuasive designs raise significant issues. AI-driven smart contracts could present information in ways that subtly influence consumer choices, steering them towards less favourable terms without explicit coercion. For instance, an AI-powered contract might emphasise certain benefits while downplaying hidden costs, shaping consumer decisions through the selective presentation of terms, thereby leveraging the *framing effect*. Such persuasive techniques challenge informed consent, the principle of good faith, and professional diligence, raising concerns about the validity<sup>21</sup> and fairness of AI-driven legal agreements.

Under the UCPD, a commercial practice is deemed *unfair* - and consequently, any contract resulting from such a practice may also be considered unfair - if it is contrary to *professional diligence* and distorts consumer economic behaviour, as established by

---

<sup>17</sup> In October 2024, the EU Digital Fairness Fitness Check identified pressing concerns: dark patterns, manipulative design and data-driven personalisation tactics are exploiting cognitive vulnerabilities, while existing laws lack adequate safeguards for consumers in today's digital age. Moreover, it highlighted that smart contracts pose significant risks: reduced control, hidden biases, and challenges in complying with pre-contractual requirements. As AI becomes increasingly central to consumer transactions, updating regulatory frameworks for AI and unfair commercial practices is vital to ensure a high level of consumer protection in the digital market.

<sup>18</sup> AI's potential to understand consumers better than they understand themselves - enabled by its capacity to process vast amounts of data - exposes them to the trader's intentions, whether benevolent or exploitative. This creates a new form of power imbalance, as traders can probabilistically predict consumer behaviour and leverage this asymmetry for profit. Cf. Serge Gijrath, 'Consumer Law as a Tool to Regulate Artificial Intelligence' in Hans-W Micklitz and others, *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021) 281.

<sup>19</sup> Recital 67 DSA describes them as follows: "Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions".

<sup>20</sup> The framing effect occurs when information is presented to the consumer in a way that manipulates their perception and, consequently, their decision. For instance, this occurs when the trader highlights the benefits while obscuring the costs associated with a proposed transaction.

<sup>21</sup> If a valid contract necessitates consent, and the consumer's consent is the result of trader manipulation, can it truly be considered genuine consent - especially when the consumer might have acted differently, perhaps even choosing not to sign the contract, had there been no manipulation? Cf. Maria Arango-Kure and Marcel Garz, 'Manipulation: An integrative framework of unethical influence in marketing' (2025) 197 (5) *Journal of Business Research* 115476.



Article 5(2). Furthermore, Article 5(3) recognises the (intrinsic) vulnerability (of certain groups) of consumers, due to their cognitive or physical state (“*infirmity*<sup>22</sup>”), age, or credulity “in a way which the trader could reasonably be expected to foresee”.

In the case of dark patterns and other manipulative strategies, traders deliberately design digital choice architectures to steer consumer economic behaviour in ways that maximise business profits: consumers are viewed merely as tools to increase their wealth, deprived of their human dignity. Rather than engaging in fair competition based on the quality and price of products, businesses increasingly prioritise consumer manipulation as a *competitive advantage*<sup>23</sup>. As a result, market success is no longer determined by the superior value of a product, but rather by the trader’s ability to exploit consumer vulnerabilities, thereby shifting the competitive market away from its foundational principles of transparency and informed consumer choice.

This critical situation highlights the pressing need for a harmonised EU legal framework that explicitly acknowledges the importance of behavioural sciences in interpreting and applying consumer protection norms<sup>24</sup>.

Indeed, a behaviourally informed interpretation of the UCPD should consider traders’ use of AI-driven smart contracts as an unfair commercial practice, *when* the AI system integrated into the smart contract has the purpose or material effect of manipulating consumers to the trader’s advantage, through the dynamic adjustment of the contract’s design based on real-time behavioural and personal data, by:

- a) Distorting consumer economic behaviour, especially through the exploitation of their vulnerabilities - Article 5;
- b) Deceiving consumers through the overall presentation of contractual information, by leveraging, e.g., the framing effect - Article 6;
- c) Impeding rational decision-making, by failing to clearly present relevant information - Article 7;
- d) Impairing the “consumer’s freedom of choice or conduct” through undue influence, by adopting, e.g., dark patterns - Article 8.

On the other hand, Article 3(1) UCTD explicitly states that a term is *unfair* if it is contrary to good faith and “causes a significant imbalance in the parties’ rights and obligations” at the expense of consumer well-being, when it is not individually negotiated.

---

<sup>22</sup> Emphasis added.

<sup>23</sup> As highlighted by Jon D Hanson & Douglas A Kysar, ‘Taking Behavioralism Seriously: Some Evidence of Market Manipulation’ (1999) 112 Harv. L. Rev. 1420: “Once one accepts that individuals systematically behave in nonrational ways, it follows from an economic perspective that others will exploit those tendencies for gain”. Consequently, it is fundamental that legal frameworks adequately address the risk of consumer manipulation. See Ryan Calo, ‘Digital Market Manipulation’ (2014) 82(4) The George Washington L. Rev. 995, 1000-1001.

<sup>24</sup> Regarding the need for a new interpretation of the UCPD that takes into account the consumer decision-making process and a behavioural law and economics approach, see, e.g., Anne-Lise Sibony, ‘Can EU Consumer Law Benefit from Behavioural Insights? An Analysis of the Unfair Practices Directive’ (2014) 6 European Journal of Private Law 901-942.

AI-driven smart contracts are forms of *contracts of adhesion*<sup>25</sup>: the contract is drafted by the trader - who predetermines the code and the AI system that operates within it, adjusting contract terms - whereas the consumer merely adheres to unilaterally drafted legal terms and conditions<sup>26</sup>. When a trader designs the contract with the sole intent of manipulating consumer behaviour, such conduct runs counter to the principle of good faith<sup>27</sup>. Indeed, this principle imposes upon parties a standard of conduct inspired by an ideal of loyal cooperation - one that weighs even more heavily on the trader, given the contractual power imbalance that physiologically characterises B2C contractual relationships.

Moreover, Article 4(1) establishes that the *unfairness assessment* shall include “all the circumstances attending the conclusion of the contract”. In this context, AI-driven smart contracts deserve special scrutiny. These technologies - capable of knowing consumers better than they know themselves, thanks to AI-enhanced analyses of consumer behavioural profiles<sup>28</sup> - may be designed in ways that push consumers towards agreeing to “individually negotiated” clauses, thereby blurring the line of authentic consent<sup>29</sup>. If consumers are behaviourally nudged into accepting binding terms by bypassing their conscious deliberation, can we still speak of genuine consent? And if so, to what extent? If the answer is negative, then no valid agreement has been reached, and such clauses should be considered legally ineffective<sup>30</sup>.

Finally, if we adopt a behaviourally informed approach to the interpretation of the UCTD as well<sup>31</sup>, we should not hesitate to consider unfair any term that causes a significant imbalance to the detriment of the consumer, when it results from AI-enhanced behavioural manipulation that exploits information, cognitive, and digital consumer vulnerabilities. As a consequence, such terms should not be considered binding, and the contract should be balanced - “if it is capable of continuing in existence without the unfair terms<sup>32</sup>” - by recognising as effective only those terms and conditions that the consumer would have agreed to in the absence of digital manipulation.

---

<sup>25</sup> Cf. Oscar Borgogno, ‘Usefulness and Dangers of Smart Contracts in Consumer Transactions’ in Larry A DiMatteo and others (eds), *Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 294.

<sup>26</sup> *Rectius*: the consumer agrees to enter into a legal agreement whose terms are generated and adjusted by an AI system integrated into the smart contract’s code, as implemented by the trader.

<sup>27</sup> On the other hand, in this writer’s view, the use of AI within a smart contract may be consistent with the principle of good faith where behavioural profiling is employed to nudge consumers towards choices that genuinely serve their interests - provided that the AI system respects consumer autonomy.

<sup>28</sup> Stefano Faraoni, ‘Persuasive Technology and computational manipulation: hypernudging out of mental self-determination’ (2023) 6 *Front. Artif. Intell.* 2.

<sup>29</sup> On the subtle strategies companies may employ to obtain consent manipulatively, see e.g. Neil Richards and Woodrow Hartzog, ‘The Pathologies of Digital Consent’ (2019) 96(6) *Washington University Law Review* 1489. For the reasons why manipulated consent should not count as proper consent, see David Alm, ‘Manipulation, Responsibility and Rights’ (2013) 47 *J Value Inquiry* 4-10.

<sup>30</sup> Faraoni (n 28) 7-11.

<sup>31</sup> See Aleksa Radonjić, ‘Behavioral approach to unfair terms and conditions in EU consumer law’ (2018) 62(8) *Strani pravni zivot* 7-21.

<sup>32</sup> Article 6(1) UCTD.



In conclusion, AI-driven smart contracts challenge the future-proof nature of the UCPD and UCTD. Since these directives were not designed with AI technologies in mind, it is worth questioning whether they are capable of adequately protecting consumers in the AI era. While their application to AI contexts can be extended through an evolutive interpretation, legislative updates may be necessary to fully address the nuanced interactions between AI and consumers in the contractual realm. At the same time, it is important to recognise that AI can also play a positive role in enhancing consumer protection, through consumer-centric applications<sup>33</sup> designed to ensure compliance with EU law, by proactively flagging or blocking potential violations before harm occurs and explaining where and why such breaches have been detected<sup>34</sup>.

## 2.2 The role of the AI Act

The AI Act plays a critical role in addressing manipulation risks<sup>35</sup>, highlighting the vital need to ensure that AI systems and applications are *human-centric*<sup>36</sup> and respectful of *human dignity*<sup>37</sup> and *personal autonomy*<sup>38</sup>. At its core, this regulation aims to ensure that AI is designed and employed in a manner that serves people and foster their well-being<sup>39</sup>. To achieve this goal, it adopts a *risk-based approach*, which categorises AI systems into four risk categories - *unacceptable*, *high*, *limited*, and *minimal* - and follows the motto: “the higher the risk, the stricter the rules<sup>40</sup>”.

Given the potential behavioural manipulation risks posed by AI-driven smart contracts, a critical question arises:

- Should AI-driven smart contracts be considered high-risk AI systems or prohibited AI practices under the EU AI Act?

---

<sup>33</sup> Marco Lippi and others, ‘Consumer protection requires artificial intelligence’ (2019) 1 Nature Machine Intelligence 168-169.

<sup>34</sup> See, e.g., the Claudette Project, “a research project aiming at automation of personal data and consumer law enforcement using machine learning”: <<http://claudette.eui.eu/index.html>> accessed 28 May 2025. Cf. Federico Ruggieri and others, ‘Detecting and explaining unfairness in consumer contracts through memory networks’ (2022) 30 Artificial Intelligence and Law 59-92.

<sup>35</sup> Particularly, Recital 28 AI Act acknowledges that AI “can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices”. Recital 29 addresses “AI-enabled manipulative techniques” that “can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices”.

<sup>36</sup> Recital 1 and Article 1(1) AI Act.

<sup>37</sup> The §11 Asilomar AI Principle - part of a set of guidelines developed during the 2017 Asilomar conference, which convened experts in AI, economics, law, ethics, and philosophy to discuss beneficial AI - states that “AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity”: <<https://futureoflife.org/open-letter/ai-principles/>> accessed 28 May 2025. This principle supports the argument that a just legal framework should promote human-centric AI and allow only such systems to be deployed and maintained in real-world applications.

<sup>38</sup> Recital 27 AI Act.

<sup>39</sup> *ibid.*

<sup>40</sup> Martin Ebers, ‘Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU’s AI Act’ (2025) 16 (2) European Journal of Risk Regulation 684-703.

As previously discussed, these technologies can potentially distort consumer behaviour. To determine their appropriate regulatory classification, it is essential to evaluate the risks they pose.

Article 5 AI Act establishes that prohibited AI practices are those that pose an *unacceptable risk*<sup>41</sup>. The relevant prohibitions include:

1. Subliminal techniques *beyond* a person's consciousness, or *purposefully* manipulative or deceptive techniques: AI systems "with the *objective*, or the *effect* of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision<sup>42</sup>". Moreover, to be prohibited, these AI practices must cause individuals to make a decision that - in the absence of such practices - they would not have made<sup>43</sup>;
  2. Exploitation of vulnerabilities: AI systems that exploit people's vulnerabilities "with the objective, or the effect, of materially distorting" the vulnerable person's behaviour.
- In both cases, to be prohibited, the AI practice should:

- a) cause significant harm, or
- b) be reasonably likely to cause significant harm<sup>44</sup>.

Consequently, AI-driven smart contracts that are designed to - or materially have the effect to - target and exploit (digitally and cognitively) vulnerable consumers, and (are reasonably likely to) cause *significant harm*<sup>45</sup> should be considered prohibited, under Article 5.

On the other hand, it is more plausible that they may fall under the high-risk category, as defined in Article 6(2) and Annex III. Article 6(2) refers to Annex III, which classifies certain AI systems as high-risk, in addition to those classified as such by Article 6(1).

In particular, Annex III(1) classifies as high-risk AI systems those that are listed in the area of biometrics<sup>46</sup>. Within the context of AI-driven smart contracts, two categories are specifically relevant:

---

<sup>41</sup> Recital 179 AI Act.

<sup>42</sup> Article 5(a) AI Act. Emphasis added.

<sup>43</sup> This formulation strongly echoes the provisions of the UCPD regarding: 1) the unfairness of a commercial practice, Article 5(2b); 2) misleading actions, Article 6(1); 3) misleading omissions, Article 7(1); 4) aggressive commercial practices, Article 8(1).

<sup>44</sup> Whenever an AI system processes consumers' personal data to behaviourally manipulate them against their own well-being - thereby partially or entirely impeding conscious decision-making - the practice itself constitutes a harm to, or a threat against, human autonomy. Cf. Shoshana Zuboff, 'The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power' (PublicAffairs 2019) 127.

<sup>45</sup> The European Commission, Brussels, 4.2.2025, C(2025) 884 final, ANNEX, 28, highlighted that the concept of harm includes "physical, psychological, financial, and economic harms that may compound with broader societal harms in certain cases".

<sup>46</sup> The notion of "biometric data" under the EU AI Act should be interpreted consistently with the definitions provided in Article 4(14) GDPR, Article 3(18) of Regulation (EU) 2018/1725, and Article 3(13) of Directive (EU) 2016/680, as explicitly referenced in Recital 14 of the AI Act. These instruments uniformly define biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".



- a) “AI systems intended to be used for biometric categorisation<sup>47</sup>”;  
b) “AI systems intended to be used for emotion recognition<sup>48</sup>”.

Moreover, Article 6(3) specifies that for an AI system to be labelled as high-risk, it must pose “a *significant* risk of harm to the health, safety, and fundamental rights of natural persons<sup>49</sup>”, including “materially influencing the outcome of decision making”. However, if the AI system employs biometric categorisation or emotion recognition, performing the profiling of consumers, it “shall always be considered to be high-risk”.

Consequently, the crucial question now is:

- Except when prohibited, should AI-driven smart contracts always be classified as high-risk?

An affirmative answer to this question is the most likely. Within the EU legal framework, an AI-driven smart contract is inherently high-risk if it behaviourally profiles the consumer. For the purposes of the AI Act, profiling involves the “automated processing of personal data” to use such data, particularly for analysing or predicting personal preferences, interests, and behaviour - among other characteristics - of a natural person<sup>50</sup>, such as the consumer. Considering that the personalisation functionalities of the smart contract rely on the capabilities of the AI system, integrated into its computer code, to adapt terms and conditions for the individual person by inferring their behavioural patterns, vulnerabilities, needs, and preferences, the AI-driven smart contract is by nature high-risk under the AI Act.

### 2.3 Algorithmic Vulnerability

The evaluation of risks associated with AI systems embedded in smart contracts must also take into account the emerging dimension of *digital vulnerability*, sometimes referred to as *algorithmic vulnerability*<sup>51</sup>. This concept captures how AI-driven personalisation can exploit consumers’ cognitive biases and behavioural tendencies, thereby increasing their susceptibility to manipulation and undue influence.

In the contractual landscape, this emerging risk demands a robust regulatory response to ensure that AI-powered contracts do not become instruments of behavioural manipulation, but rather tools that empower and protect consumers. To this end, strengthening transparency obligations, prohibiting exploitative AI practices, and aligning

---

<sup>47</sup> AI used for biometric categorisation within a smart contract may process personal data to classify individuals into behavioural or psychological categories. This can inform the dynamic adaptation of contract terms, effectively tailoring the agreement on the individual consumer addressed by the contract.

<sup>48</sup> Emotion recognition AI technologies integrated into smart contracts may infer or detect a consumer’s emotional state through the analysis of personal data and their online behaviour. Such insights can be used to personalise or influence the contractual offer - for instance, by adapting terms to the consumer’s emotional context or by prompting a decision to conclude a contract based on their inner state.

<sup>49</sup> Emphasis added.

<sup>50</sup> Article 3(52) AI Act and Article 4(4) GDPR.

<sup>51</sup> Teresa Rodríguez de las Heras Ballell, ‘Digital Vulnerability and the Formulation of Harmonised Rules’ in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos 2024) 291.

AI-enhanced contracting systems with existing EU consumer protection frameworks are essential safeguards for mitigating such risks. As the EU's regulatory framework on AI continues to evolve, particular attention must be paid to the intersection of automated contracting, AI-driven personalisation, and consumer rights. This must be done in a manner that preserves space for innovation while upholding the fundamental rights of individuals.

In this context, it is critical to recognise that consumers do not always act in fully rational ways<sup>52</sup>, and that AI systems, when exploiting cognitive vulnerabilities, may amplify these irrational tendencies. Ensuring a high level of consumer protection in the digital market therefore requires that AI-driven smart contracts are designed not to take advantage of these vulnerabilities, but to guide consumers towards choices that maximise their well-being. In doing so, AI not only respects consumer autonomy but also contributes to the development of more efficient and fair markets<sup>53</sup>. A digital economy in which competition is based on the quality of goods and services - rather than on a business's capacity to manipulate consumer behaviour - is ultimately more sustainable and aligned with the broader public interest<sup>54</sup>.

The overarching objective should remain clear: AI must be designed and employed as a tool that serves humanity, ultimately fostering a fair, just and consumer-centric digital market.

### 3 Ai-Driven Smart contracts & GDPR compliance

AI-driven smart contracts rely on the processing of consumer data to function effectively, raising significant concerns regarding their compliance with the GDPR. Unlike traditional smart contracts, which operate based on predefined and immutable rules, AI-enhanced versions can analyse consumer behaviour and preferences to dynamically adjust contractual terms and conditions based on real-time personal data analysis. While this capability enhances adaptability and contract personalisation, it simultaneously introduces substantial risks of personal data exploitation<sup>55</sup>.

---

<sup>52</sup> See, e.g., Daniel Kahneman, *Thinking fast and slow* (Farrar, Straus and Giroux 2011); Richard Thaler, *Misbehaving: The Making of Behavioral Economics* (W. W. Norton & Company 2015); Oren Bar-Gill, 'Consumer Transactions' in Eyal Zamir and Doron Teichman (eds), *The Oxford Handbook of Behavioral Economics and the Law* (OUP 2014) 465-490; Botond Koszegi, 'Behavioral Contract Theory' (2014) 4 (52) *Journal of Economic Literature* 1075-1118.

<sup>53</sup> Ioannis Lianos, 'Value extraction and institutions in digital capitalism: Towards a law and political economy synthesis for competition law' (2022) 1 *European Law Open* 887-888.

<sup>54</sup> *ibid.* 869-871.

<sup>55</sup> The integration of AI into a smart contract endows it with dynamic and adaptive capabilities. Through machine learning algorithms, such contracts can autonomously modify their terms and conditions based on the behavioural profile of the consumer with whom they interact - often relying on oracles to retrieve data from external sources. In this context, the AI-driven smart contract functions as a responsive system with two core objectives: (1) to analyse and understand the consumer, and (2) to adapt contractual content accordingly. Personal data thus become the operational 'fuel' that enables the contract to achieve these aims. Cf. Mimi Zou, 'When AI Meets Smart Contracts: The Regulation of Hyper-Autonomous Contracting Systems?' in Martin Ebers and others (eds), *Contracting and Contract Law in the Age of Artificial Intelligence* (Hart 2022) 48-49.



In particular, to ensure compliance with the GDPR, AI-driven smart contracts that collect and process consumer data must adhere to the following principles:

- a) **Lawfulness, fairness, and transparency:** personal data processing must be lawful, fair, and transparent<sup>56</sup>;
- b) **Purpose limitation**<sup>57</sup>: personal data must be collected for “specified, explicit, and legitimate purposes”, and further processing is allowed only if compatible with those purposes. If further processing serves a public interest - i.e., ensuring a high level of consumer protection and market efficiency - it shall “not be considered to be incompatible with the initial purposes<sup>58</sup>”;
- c) **Data minimisation**<sup>59</sup>: personal data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed<sup>60</sup>”;
- d) **Contractual necessity:** personal data processing is lawful *if* it is “necessary for the performance of a contract to which the data subject is party<sup>61</sup>”;
- e) **Consent:** if personal data processing is based on the data subject’s (i.e., the consumer’s) consent<sup>62</sup>, the controller (i.e., the trader) must be able to demonstrate it<sup>63</sup>.

Consequently, the key question is:

- Can AI-driven smart contracts comply with the GDPR?

### 3.1 The privacy-by-design solution

The compliance of AI-driven smart contracts with the GDPR ultimately hinges on their design and implementation. A robust approach to ensuring such compliance may involve the adoption of the *privacy-by-design* approach, as enshrined in Article 25. This possible solution entails the integration of data protection principles into the architecture of the AI system that is incorporated within the smart contract itself<sup>64</sup>.

First, to comply with the principle of **lawfulness, fairness, and transparency**, a privacy-by-design model should:

- Embed explainability and interpretability mechanisms to ensure that consumers can understand how and why their data are processed. This may include the integration of explainable AI techniques that provide clear, non-technical, and accessible explanations tailored to the consumer’s level of comprehension;

---

<sup>56</sup> Article 5(1)(a) GDPR.

<sup>57</sup> Cf. W Gregory Voss, ‘Data Protection Issues for Smart Contracts’ in Marcelo Corrales Compagnucci and others (eds), *Smart Contracts: Technological, Business and Legal Perspectives* (Hart 2021) 97-98.

<sup>58</sup> Article 5(1)(b) GDPR.

<sup>59</sup> Gregory Voss (n 57) 98.

<sup>60</sup> Article 5(1)(c) GDPR.

<sup>61</sup> Article 6(1)(b). See, also, Recital 44 GDPR.

<sup>62</sup> Article 6(1)(a) GDPR.

<sup>63</sup> Article 7(1) GDPR.

<sup>64</sup> Cf. Lokke Moerel, ‘Blockchain and Data Protection’ in Larry A DiMatteo and others (eds) (n 25) 224-225.

- Provide user-friendly interfaces that enable consumers, as data subjects, to access information on the processing of their personal data and to effectively exercise their rights under Articles 13-22 GDPR.

Second, the proposed approach has the potential to enforce the **purpose limitation** principle by:

- Embedding purpose-binding protocols within AI-driven smart contracts, ensuring that data are processed solely for pre-defined contractual purposes;
- Impeding *function creep* - where data processing goes beyond its original purposes - through the incorporation of data governance mechanisms into the design of smart contracts.

Third, in relation to the principle of **data minimisation** - which requires the processing of only strictly necessary data - AI-driven smart contracts may, by their nature, risk excessive behavioural profiling and data collection. A privacy-by-design approach can mitigate this risk by:

- Preventing the processing of personal data that are not strictly relevant to achieving the contract's pre-defined purposes;
- Enforcing automatic data retention policies that restrict the unnecessary storage of personal information (storage limitation<sup>65</sup>).

Fourth, where the processing of personal data is lawful on the basis that it is strictly necessary for the performance of a contract to which the consumer is a party (**contractual necessity**), the privacy-by-design approach can support compliance by embedding the *necessity assessments* within the AI system to ensure that each instance of personal data processing is genuinely essential for the execution of the contract.

Fifth, when AI-driven smart contracts rely on **consumer consent** as the legal basis for personal data processing, the privacy-by-design approach should enhance compliance through:

- Embedding dynamic consent management mechanisms that allow consumers to review, modify, or withdraw consent at any time<sup>66</sup>;
- Providing granular consent options, enabling consumers to approve specific data processing activities while rejecting others;
- Implementing tamper-proof consent logs that document the history of consent, thereby strengthening trust, accountability, and verifiability;

---

<sup>65</sup> Article 5(1)(e) GDPR.

<sup>66</sup> Article 7(3) GDPR establishes the right for data subjects to withdraw their consent at any time. Consequently, consumers must be able to revoke consent at any point, even after the contract has been executed, provided that the data controller - i.e. the trader - continues to maintain access to their personal data. In the context of AI-driven smart contracts, which are typically designed to automatically execute once the "if" condition is met, consumers must have the ability to review, modify, or withdraw their consent where their personal data continues to be retained post-execution. Additionally, consumers should be able to determine the specific purposes for which their data is used - whether to facilitate future transactions or for any other reason. Ultimately, the privacy-by-design approach seeks to empower consumers, enabling them to maintain control over the use of their personal data throughout the entire lifecycle of the contract.



- Ensuring that any secondary use of data (e.g., for AI model training) is subject to explicit consumer consent<sup>67</sup> or to a legitimate interest assessment<sup>68</sup>.

### 3.2 Automated decision-making

Another key legal question is whether AI-driven smart contracts qualify as *automated decision-making* (ADM) under Article 22 GDPR<sup>69</sup>. Article 22(1) states that the “data subject shall have the *right not to* be subject to a decision based solely on automated processing, including profiling, which produces legal effects<sup>70</sup>” that concern them. AI-driven smart contracts fall within this category<sup>71</sup> because they autonomously adjust contract terms and conditions based on real-time consumer data analysis - which may include behavioural profiling - thereby tailoring contractual obligations to the individual consumer they address.

As previously discussed, these contracts typically function as *contracts of adhesion*, where the sole decision consumers face is *whether* they want to enter into the agreement, without any (or significant) negotiation power. Consequently, consumers are asked to make a binary decision: to accept or reject the contract as is. If they accept, they enter into a legal agreement that has been tailored for them. The AI system within the smart contract has processed their data and dynamically shaped the contract, determining an automated decision that produces legal effects concerning them - e.g. by establishing the reciprocal contractual obligations.

However, Article 22(2)(a) provides an exemption to the applicability of the first paragraph if the decision “is necessary for entering into, or performance of, a contract between the data subject and a data controller”. In this context:

- The data subject is the consumer, whose personal data are collected and processed by the AI system embedded within the smart contract;
- the data controller is the trader, who “determines the purposes and means of the processing of personal data<sup>72</sup>”.

For instance, an AI-driven smart contract may determine whether the consumer can enter into the contract - for example, by assessing their creditworthiness. Moreover, the ADM process could shape contractual obligations, thereby directly involving the contract’s performance. In this context, the ADM is integral to the contract’s performance, as it dynamically determines the content of the reciprocal obligations and, once the encoded condition is met (e.g., the consumer pays the price), executes them automatically.

---

<sup>67</sup> Article 6(1)(a) GDPR.

<sup>68</sup> Article 6(1)(f) GDPR.

<sup>69</sup> See Michèle Finck, ‘Smart Contracts and Article 22 GDPR’ (2019) 9 (2) International Data Privacy Law 82-84.

<sup>70</sup> Emphasis added.

<sup>71</sup> Cf. Olumide Babalola, ‘Viewing Smart Contracts Through GDPR Lenses’ (2022) 10(4) Global Journal of Politics and Law Research 78.

<sup>72</sup> Article 4(7) GDPR.

However, under the European Data Protection Board's narrow reading of *necessity*, the question is whether "other effective and less intrusive means<sup>73</sup>" could be adopted in place of ADM to achieve the contractual purposes. Controllers "must be able to show that this type of processing is necessary, taking into account whether a less privacy-intrusive method could be adopted<sup>74</sup>". A stricter interpretation may, therefore, exclude that the ADM is necessary for the performance of AI-driven smart contracts, on the basis that a traditional, entirely human-made contract remains a viable alternative. Yet, AI integration into the smart contract's code enables what humans cannot achieve (within reasonable timeframes), such as analysing consumer data in real time to deliver a contract individually tailored to the specific characteristics of the targeted consumer - which is the very reason why traders opt for this kind of technologies to shape their legal agreements. In sum, while a less privacy-intrusive method could theoretically be adopted, in the context of AI-driven smart contracts, such an alternative would undermine the defining contractual objective - the dynamic, real-time tailoring of terms and conditions to the individual consumer - and thus it should not be considered a functionally equivalent "means to achieve the same goal<sup>75</sup>".

Additionally, as an alternative to the *necessity assessment* required by Article 22(2)(a), another exemption to the first paragraph is provided under letter (c), which requires that the decision "is based on the data subject's explicit consent".

In both cases, the trader must "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests<sup>76</sup>". At minimum, the following data subject's rights must be guaranteed:

- the right to obtain human intervention in the decision-making process;
- the right to express their point of view;
- the right to contest the decision<sup>77</sup>.

Furthermore, Article 22(4) establishes that decisions "referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place".

Article 9(1) categorises *biometric data* - defined as data "resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person<sup>78</sup>" - as a special category of personal data whose processing is, in principle,

---

<sup>73</sup> European Commission, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 23.

<sup>74</sup> *ibid.*

<sup>75</sup> *ibid.*

<sup>76</sup> Article 22(3) GDPR.

<sup>77</sup> *ibid.*

<sup>78</sup> See (n 46).



prohibited. AI-driven smart contracts may, indeed, process this type of data to behaviourally profile consumers and, consequently, draft the contract accordingly.

However, this prohibition is not absolute. It does not apply when “the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject<sup>79</sup>”. As a result, if the consumer has *explicitly* agreed to the processing of their data - for example, to allow the AI system to adjust the contract to better serve the consumer’s interests - the prohibition is lifted. It is crucial, however, that the explicit consent relates to one or more clearly defined purposes.

Additionally, the prohibition does not apply *if* the processing of special categories of personal data “is necessary for reasons of substantial public interest<sup>80</sup>”. The concept of public interest may include the objective of ensuring a high level of consumer protection, particularly when the AI-driven smart contract is designed to maximise the consumer’s well-being, autonomy, and rights.

In this case, it is essential:

- a) a proportionality assessment to the aim pursued;
- b) respect for “the essence of the right to data protection<sup>81</sup>”;
- c) the safeguarding of the data subject’s fundamental rights and interests through “suitable and specific measures<sup>82</sup>”.

### 3.3 A legal crossroads

Ultimately, the compliance of AI-driven smart contracts with the GDPR depends on their design: how they are conceived and implemented determines their legitimacy. Moreover, assessing their actual purposes is essential to evaluate their compatibility with the EU legal framework.

If designed and implemented in a consumer-friendly manner, aiming at achieving consumer protection goals - such as safeguarding consumer rights, privacy, and autonomy - AI-driven smart contracts can contribute to the supranational objective of ensuring a high level of consumer protection.

Furthermore, if these technologies are designed in a way that fosters consumer trust in AI-driven transactions and the digital market, a privacy-by-design approach may also serve as a tool to enhance market efficiency. By protecting consumers - for instance, by nudging them towards optimal decision-making and more informed contractual choices<sup>83</sup> - the market itself is protected, as an efficient market depends on efficient consumers.

---

<sup>79</sup> Article 9(2)(a) GDPR.

<sup>80</sup> Article 9(2)(g) GDPR.

<sup>81</sup> *ibid.*

<sup>82</sup> *ibid.*

<sup>83</sup> Cass R Sunstein, ‘The Ethics of Nudging’ (2015) 32(2) Yale Journal on Regulation 434.

However, to achieve these goals, it is essential that consumers trust these technologies. Such trust can only be established if consumers feel that AI-driven smart contracts process their personal data in ways that comply with the GDPR and genuinely serve their interests.

Additionally, concerning the relationship between consumer protection law and data protection law, it is important to note that their boundaries are becoming increasingly blurred in our digitalised world<sup>84</sup>. When consumers engage in the digital market, they are not only potential contracting parties but also data subjects<sup>85</sup>. Therefore, ensuring that their personal data are processed lawfully and in their best interests is a vital condition for safeguarding consumer protection against data exploitation and digital manipulation<sup>86</sup>.

A key question remains: should the EU introduce a dedicated regulation to address the unique opportunities and risks posed by AI systems and their integration into smart contracts, particularly in the context of personal data? If their use becomes more widespread in the future, the answer seems increasingly likely to be affirmative. Given their adaptive and dynamic nature, a specific regulation could provide legal certainty, balancing innovation with the principles and objectives of consumer and data protection<sup>87</sup>.

#### 4 Ai-Driven Smart contracts & the DSA

Online platforms may provide user-friendly web or mobile interfaces where consumers can access and interact<sup>88</sup> with AI-driven smart contracts. In this context, another relevant EU regulation is the DSA, which establishes a comprehensive legal framework for online platforms. While it does not directly regulate AI-driven smart contracts, it applies when these contracts are hosted, promoted, or executed via such digital environments.

Particularly, the DSA introduces obligations concerning three key areas, which are relevant to ensuring that AI-driven smart contracts contribute to achieving a high level of consumer protection: 1) platform liability, 2) content moderation, and 3) algorithmic transparency and fairness.

---

<sup>84</sup> Natali Helberger, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54(5) *Common Market Law Review* 1428.

<sup>85</sup> *ibid* 1430-1431.

<sup>86</sup> *ibid* 1458.

<sup>87</sup> It is essential that any future regulatory framework addressing AI and its integration into smart contracts not only mitigates the specific risks posed to personal data but also fosters human-centric innovation. Striking this balance requires a normative approach that ensures innovation is directed towards serving humankind - just as the processing of personal data must, according to the values enshrined in Recital 4 GDPR. In this light, innovation and data protection are not opposing forces but can be aligned through a legal framework that channels technological progress towards human- and consumer-centric goals. In this regard, a future-proof and innovation-oriented regulation should be capable of actively reinforcing GDPR compliance by harnessing the potential of AI within the evolving context of AI-driven contracting. See Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 4 *European Data Protection Law Review* 32-35.

<sup>88</sup> Cf. Folkert Wilman and others, 'General Provisions' in Folkert Wilman and others (eds), *The EU Digital Services Act* (OUP 2024) 16.



#### 4.1 Platform liability

The central question of this sub-paragraph is whether online platforms - that facilitate AI-driven smart contract transactions - could be held liable for non-compliant or harmful contractual terms and conditions under the DSA. Indeed, online platforms can serve as marketplaces - virtual spaces where AI-driven smart contracts are hosted and promoted, enabling consumers to enter into such legal agreements<sup>89</sup>. Consequently, if an AI-driven smart contract contains unfair terms, constitutes an unfair commercial practice, or violates the GDPR, should the platform hosting it be held liable<sup>90</sup>?

Under Article 3(i) DSA, online platforms are *hosting services* “that, at the request of a recipient of the service,” store and disseminate information to the public. In particular, the recipient of the service may be a *trader*<sup>91</sup> - who advertises or sells products and services online - or a *consumer*<sup>92</sup> - who makes purchases online or views ads on social media platforms. In this context, AI-driven smart contracts can be hosted by an online platform, where traders can incentivise - and consumers can choose to enter into - this type of legal agreements<sup>93</sup>.

According to Article 6(1), hosting service providers - for example, those who, enable traders to upload their smart contracts onto online platforms and consumers to visualise and agree to these contracts - are not liable “for the information stored at the request of a recipient of the service”, provided that they are unaware that the content hosted is illegal or, once aware, act expeditiously “to remove or to disable access” to it.

However, this exemption from liability does not apply, and the hosting service provider can be held liable in the following cases:

- 1) When “the recipient of the service is acting under the authority or the control of the provider” - Article 6(2);
- 2) If the online platform allows B2C distance contract transactions<sup>94</sup> in such a way that it misleads the average consumer into believing that the information or the product/service (the object of the transaction) is being provided by the online platform or by a recipient of the service acting under its authority or control<sup>95</sup> - Article 6(3).

---

<sup>89</sup> Cf. *ibid.* 39-40.

<sup>90</sup> According to Article 3(h) DSA, “illegal content” refers to any information that is not in compliance with EU or domestic law. Accordingly, contractual clauses embedded in AI-driven smart contracts - when hosted and promoted by online platforms - may qualify as illegal content if they infringe the UCPD, UCTD, GDPR or AI Act. See *ibid.* 38-39.

<sup>91</sup> Article 3(f) DSA.

<sup>92</sup> Article 3(c) DSA.

<sup>93</sup> Cf. (n 88) 34.

<sup>94</sup> Indeed, B2C distance contract transactions fall within the scope of the DSA when concluded on online platforms. These platforms facilitate interaction between traders and consumers: the former promote and offer contracts, which the latter may choose to enter into. *Ibid.* 42.

<sup>95</sup> Under Article 31(1) DSA, online platforms providers - excluding micro and small enterprises - that facilitate B2C distance contract transactions must ensure that the design and organisation of their online interface enable traders “to comply with their obligations regarding precontractual information, compliance and product safety information”. More broadly, they must comply with the provisions set out in Articles 29-32.

Additionally, Article 7 clarifies that if the intermediary service provider has - in good faith and diligently - voluntarily investigated or taken other measures to detect, identify, remove, or disable access to illegal content, the exemptions from liability set out in Article 6 may still apply.

This framework implies that, when an illegal AI-driven smart contract is hosted and/or promoted on an online platform, the platform provider may be held liable in the following cases:

1. **Failure to act:** the provider fails to remove the contract from the platform or disable consumer access to it, upon obtaining knowledge or awareness of the illegal content - namely, the legal agreement;
2. **Misleading design:** the online platform's design leads the average consumer to believe that the AI-driven smart contract, which constitutes a distance contract, is being offered and/or promoted by the online platform itself or by a recipient of the service acting under the provider's authority or control;
3. **Traders acting under the provider's control or authority:** the trader is acting under the authority or control of the provider<sup>96</sup> - i.e. the online platform provider and the trader are not independent entities.

In this context, if an online platform hosts or promotes AI-driven smart contracts that are unlawful - for instance, because they contain unfair terms in violation of the UCTD, constitute an unfair commercial practice under the UCPD, or process and collect data in a way that is not compliant with the GDPR - it is obliged to remove or restrict access to such contracts once it becomes aware of the illegal content on its platform.

Moreover, if the platform at issue is a very large online platform (VLOP) under Article 33, it faces additional duties, including conducting risk assessments and implementing risk mitigation measures<sup>97</sup>. Article 34(1) further establishes that VLOP providers have an obligation to "diligently identify, analyse, and assess any systemic risks", including:

- 1) "the dissemination of illegal content through their services<sup>98</sup>";
- 2) "any actual or foreseeable negative effect for the exercise of fundamental rights" - in particular, the fundamental rights to:
  - Human dignity - which is at risk when consumers face digital manipulation and are treated merely as tools to increase corporate profits at the expense of their well-being;
  - The protection of personal data - which requires strict compliance with the GDPR;
  - Non-discrimination - which is threatened when the AI system embedded in the smart contract is biased, leading to suboptimal and harmful decision-making;

---

<sup>96</sup> Article 6(2) DSA.

<sup>97</sup> Sebastian K Stiković, 'The EU's Digital Services Act and Its Impact on Online Platforms' (2024) 85 European Union Law Working Papers 65-67.

<sup>98</sup> In the context of AI-driven smart contracts, they may be deemed illegal content when they do not comply with EU law (e.g., the UCTD, UCPD, GDPR, or AI Act).



- A high level of consumer protection - an objective that may be fully achieved when contracts are designed to concretely safeguard consumers from their vulnerability and guide them towards efficient economic decisions, thereby not impairing - but strengthening - their rationality, while respecting their autonomy.

Additionally, Article 35 states that VLOP providers have the duty to adopt “reasonable, proportionate, and effective mitigation measures”, which must be “tailored to the specific systemic risks” that they address<sup>99</sup>.

In sum, online platforms - particularly VLOPs - can be held liable if they knowingly host and/or promote unlawful AI-driven smart contracts, fail to act upon becoming aware of such illegal content, or design their services in a manner that misleads consumers about the platform’s role in providing these contracts. This framework contributes to ensuring that AI-driven smart contracts are designed to achieve a high level of consumer protection. Therefore, if a contract fails to be consumer-friendly and foster rational decision-making - by exploiting consumers’ vulnerability, manipulating their behaviour, or violating data protection rules - the platform must remove or disable consumer access to it. Failure to do so may result in liability for the platform itself.

#### 4.2 The content moderation challenge

To comply with the DSA, the overall architecture of online platforms must be designed in a user-friendly manner, enabling anyone to report content - including AI-driven smart contracts - that they consider illegal<sup>100</sup>. This implies that platforms must establish mechanisms that allow consumers to flag unfair contract terms, dark patterns, and other forms of digital manipulation they believe they have encountered<sup>101</sup>. As a result, if such reports are substantiated<sup>102</sup> - demonstrating that the contract, hosted by the online platform, contains terms that violate consumer protection laws - and the platform reaches the same conclusion as the reporting consumer, determining that the contract is unlawful, then it has a duty to prevent further consumer interaction with it.

Providers, in turn, must notify the *flagger* of their decision, “providing information on the possibilities to redress in respect of that decision<sup>103</sup>”. If providers conclude that the content is illegal, they must notify the recipient of the service - the trader, in the case of B2C AI-driven smart contracts - explaining the reasons behind their decision<sup>104</sup>, particularly where on the online platform:

---

<sup>99</sup> See (n 97) 68.

<sup>100</sup> Article 16(1) DSA. Cf. Jorge M Carvalho, ‘Introduction to the Digital Services Act, Content Moderation and Consumer Protection’ (2021) 3 *Revista de Direito e Tecnologia* 92-94.

<sup>101</sup> A contractual clause that has been autonomously modified by an AI system integrated into the smart contract may also qualify as illegal content, where such modifications rely on the processing of personal data in breach of the GDPR.

<sup>102</sup> Article 16(2)(a) DSA.

<sup>103</sup> Article 16(5) DSA.

<sup>104</sup> Article 17(1) DSA.

- a) the AI-driven smart contract has been removed, demoted, or made inaccessible to consumers<sup>105</sup>;
- b) the trader's account has been suspended or terminated<sup>106</sup>.

Moreover, Article 34 requires VLOP providers to assess whether and how their content moderation systems influence systemic risks<sup>107</sup>, while Article 35 demands that they tailor mitigation measures to such risks, “adapting content moderation processes, including [...] where appropriate, the expeditious removal of, or the disabling of access to, the content notified<sup>108</sup>”.

The primary challenge lies in implementing efficient content moderation mechanisms that allow consumers to report non-compliant contracts. At the same time, providers must proactively neutralise illegal contracts once they become aware of them. Additionally, VLOP providers must identify systemic risks and tailor their content moderation mechanisms to address these risks more effectively. Ultimately, this framework contributes to ensuring contract compliance with EU law.

However, moderating AI-driven smart contracts may be particularly challenging, as they operate autonomously and execute transactions in real time, making pre-emptive intervention difficult. Consequently, providers must assess in advance whether the AI embedded within a smart contract is capable of dynamically modifying contractual terms and conditions in a manner that renders the contract non-compliant with EU law.

In conclusion, within the context of AI-driven smart contracts, content moderation plays a crucial role in fostering a high level of consumer protection. By preventing online platforms from hosting AI-driven smart contracts that violate consumer and data protection laws, and by enabling consumers to report contracts that they perceive as unlawful, content moderation contributes to a more transparent and consumer-friendly digital market<sup>109</sup>.

#### 4.3 Algorithmic accountability & transparency obligation

To ensure a high level of consumer protection, recommender systems employed by online platforms can play a crucial role. Specifically, online platforms may prioritise certain AI-driven smart contracts, displaying them more prominently and thereby

---

<sup>105</sup> Article 17(1)(a) DSA.

<sup>106</sup> Article 17(1)(d) DSA. In particular, under Article 23(1), if the *flagged* trader usually provides “manifestly illegal content”, the provider is required to suspend them “for a reasonable period of time and after having issued a prior warning”.

<sup>107</sup> Article 34(2)(b) DSA.

<sup>108</sup> Article 35(1)(c) DSA.

<sup>109</sup> As set out in Article 1(1) DSA, the Regulation aims to safeguard the respect of consumer protection principles as a means of ensuring the proper functioning of the internal market. Indeed, the two objectives are closely intertwined: (1) an efficient market requires efficient economic agents; (2) consumers are economic agents who need a “safe, predictable, and trusted online environment” to thrive and make efficient economic decisions. As a result, a regulation that protects consumers ultimately safeguards the market as well. The DSA seeks to achieve this goal while also fostering innovation.



directing consumer attention towards specific legal agreements over others. Their capacity to steer consumer choices in ways that align with consumers' best interests is vital to enhancing individual well-being and, ultimately, to ensuring the proper functioning of the internal market<sup>110</sup>.

Article 27 mandates that, when online platform providers utilise recommender systems, they must clearly disclose the main parameters used<sup>111</sup> and the options available “for the recipients of the service to modify or influence those main parameters”. Moreover, providers must enable them to select and modify “at any time their preferred option<sup>112</sup>”, thereby ensuring greater autonomy over how content is ranked and presented to them.

Under Article 34(2)(a), VLOP providers are also required to assess how the design of their recommender systems impacts systemic risks. Additionally, as part of their mitigation obligations, these systems must be tested and adapted to neutralise such risks<sup>113</sup>.

In the context of AI-driven smart contracts, this implies that providers must enable consumers to choose how contracts are ranked and prioritised on online platforms. Moreover, VLOP providers must ensure that their recommender systems adequately protect consumers from contracts that are illegal or detrimental to their well-being<sup>114</sup>.

However, an open question remains regarding the efficacy of Article 27 in ensuring a high level of consumer protection. While it empowers consumers to adjust their recommender system preferences, a more effective regulatory approach may require online platform providers to deploy recommender systems that proactively identify and suggest contracts most suitable for the individual consumer. An efficient recommender system should not only highlight the most appropriate contracts but also present them in a consumer-friendly manner - clearly comparing key elements, highlighting relevant information, and using intelligible and accessible language<sup>115</sup>. When combined with adequate human oversight to monitor and refine their performance, such systems could significantly enhance consumer protection. They would help guide consumers towards AI-

---

<sup>110</sup> Recommender systems can ultimately serve as tools to enhance consumer decision-making, by directing attention to content that best satisfies individual needs and preferences. In the contractual context, this entails matching consumers with the contract - or set of contracts - most closely tailored to their specific circumstances and interests. Cf. Laurens Naudts and others, ‘A Right to Constructive Optimization: A Public Interest Approach to Recommender Systems in the Digital Services Act’ (2025) 48(3) *Journal of Consumer Policy* 269.

<sup>111</sup> Article 27(2) DSA further clarifies that providers must at least explain the criteria that determine the “information suggested to the recipient of the service” and “the reasons for the relative importance of those parameters”.

<sup>112</sup> Article 27(3) DSA.

<sup>113</sup> Article 35(1)(d).

<sup>114</sup> It has been illustrated that, since recommender systems effectively determine which information reaches consumers and captures their attention, VLOP providers bear a public duty to design and implement these systems in ways that serve the best interests of consumers and promote overall societal well-being. See (n 110) 6.

<sup>115</sup> Regarding the importance of contractual information design in improving consumer understanding of their rights and obligations - thereby enhancing their decision-making and economic choices - see Joasia Luzak and others, ‘ABC of Online Consumer Disclosure Duties: Improving Transparency and Legal Certainty in Europe’ (2023) 46 *Journal of Consumer Policy* 328-329.

driven smart contracts that align with their best interests, while shielding them from potentially harmful legal agreements.

## 5 Liability: centralised vs. decentralised platforms

The issue of liability in the context of AI-driven smart contracts varies significantly depending on whether they operate within centralised or decentralised ecosystems.

In centralised platforms, the liability issue is more straightforward. In this context, the following can be held liable:

1. The online platform provider under the DSA<sup>116</sup>;
2. The trader offering the AI-driven transaction, if the contract:
  - a. Contains unfair terms under the UCTD<sup>117</sup>;
  - b. Constitutes an unfair commercial practice under the UCPD<sup>118</sup>;
  - c. Violates the GDPR<sup>119</sup>;
  - d. Violates the AI Act<sup>120</sup>.

In decentralised platforms, the situation is far more complex due to the absence of a central controlling entity. While the trader can be held liable, as in centralised platforms, there is no platform provider to be held liable under the DSA, since AI-driven smart contracts are hosted and/or promoted in an environment without a central authority. Moreover, the pseudonymous and decentralised nature of these platforms makes it difficult to identify and track traders<sup>121</sup>, complicating the enforcement of consumer protection laws<sup>122</sup>. To address this issue, future regulations could mandate that, in the context of B2C contractual relationships, traders always remain identifiable, ensuring consumers have effective access to redress mechanisms in the event of harm<sup>123</sup>.

Moreover, it is important to note that traders should not be considered liable only when acting with fault or intent. When the AI embedded in a smart contract causes harm to the consumer, liability should be attributed to the trader<sup>124</sup> - namely, the party who integrated the AI system into the contract - even if the harm was not intentional or foreseeable. This reflects the reality that even diligent traders and AI developers may not be able to anticipate all outcomes of autonomous AI decision-making<sup>125</sup>. For this reason, to guarantee a high level of consumer protection, a strict liability regime may be justified: one that assigns responsibility to the trader simply by virtue of deploying the AI system

---

<sup>116</sup> See paragraph 4.1.

<sup>117</sup> See paragraph 2.1.

<sup>118</sup> *ibid.*

<sup>119</sup> See paragraph 3.

<sup>120</sup> See paragraph 2.2.

<sup>121</sup> Cf. Alesia Zhuk, 'Beyond the blockchain hype: addressing legal and regulatory challenges' (2025) 5 SN Social Sciences 11, 24.

<sup>122</sup> Cf. *ibid.* 21-23.

<sup>123</sup> Cf. (n 1) 105.

<sup>124</sup> Cristina Poncibò, 'Remedies for Artificial Intelligence' in Martin Ebers and others (eds) (n 55) 211.

<sup>125</sup> *ibid.* 212-213.



within the smart contract's code. Since the AI system itself cannot be held accountable or provide redress, liability should rest with those who profit from its use<sup>126</sup>. This, ultimately, underscores the vital importance that even in decentralised systems consumers can identify the trader and be able to seek redress from them.

Another key consideration concerns the liability of AI developers. Since the relationship between the trader and the AI provider is a B2B matter, it does not directly concern the B2C contractual relationship<sup>127</sup>. Therefore, consumers should seek reparations from the trader who offered the AI-driven smart contract, rather than from the AI provider itself.

In conclusion, while centralised platforms provide a clearer liability framework, decentralised platforms present more complex consumer protection challenges, which highlight the need for future regulatory efforts to ensure clear pathways for consumers to seek remedies in the event of harm in decentralised systems.

## 6 AI-Driven Smart Contracts Transparency

The integration of AI into smart contracts introduces a fundamental tension between automation and the consumer's right to understand how the AI decides. A key issue in this context is the opacity of AI-driven decision-making, commonly referred to as the "black-box problem", which stems from a lack of explainability and transparency in AI-generated outcomes<sup>128</sup>. Unlike traditional smart contracts - which typically operate on predefined and rule-based logic - AI-driven ones are far more complex. Most modern AI models consist of multiple layers of interconnected computational nodes - such as millions of tiny math operations. As a result, they do not follow a simple *if-then* structure; instead, they operate like a giant, tangled web of weighted probabilities, making it difficult to trace how a specific decision is reached<sup>129</sup>.

For instance, an AI-driven smart contract may be employed to assess a consumer's creditworthiness by analysing factors such as credit history, behavioural patterns (to determine whether they tend to make rational and balanced choices), financial stability, and projected future income. Based on this assessment, the AI system determines whether the consumer qualifies for a loan, the amount to be granted, and the conditions attached

---

<sup>126</sup> Baris Soyer and Andrew Tettenborn, 'Artificial intelligence and civil liability - do we need a new regime?' (2022) 30 *International Journal of Law and Information Technology* 391.

<sup>127</sup> Indeed, the B2C AI-driven smart contract gives rise to a contractual relationship between the trader and the consumer. Consequently, the consumer has no direct contact with, nor claims against, those involved in the preceding B2B relationship. However, within that B2B chain, the AI developer's fault may be relevant for questions of product liability.

<sup>128</sup> The more complex the AI embedded into the smart contract is, and the more precise its predictive capabilities are, the less explainable it becomes. In this context, there is an inherent trade-off between: 1) the performance of AI in accurately analysing consumer data and behavioural patterns, and in evaluating how contractual terms and interface design influence consumer behaviour; and 2) the explainability of the AI's outputs. As things stand, this means that optimal and efficient AI-driven smart contracts tend to function as "black boxes" by their very nature. Cf. Keri Grieman, 'Explainable AI (XAI)' in *Law, Death, and Robots* (Hart 2024) 46.

<sup>129</sup> Jens C. Bjerring, 'Deep learning models and the limits of explainable artificial intelligence' (2025) 4 (22) *Asian Journal of Philosophy* 6.

to the credit agreement<sup>130</sup>. However, if the AI denies the loan or imposes restrictive conditions without providing comprehensible reasoning, it raises a critical opacity issue, ultimately undermining consumer trust in AI-driven transactions<sup>131</sup>. This lack of transparency prevents consumers from understanding, trusting, or contesting decisions that may have significant implications for their rights and obligations<sup>132</sup>.

The following sub-paragraphs aim to critically assess this issue and explore potential solutions by addressing the following research question:

- Can AI-driven smart contracts be designed to ensure transparency and trustworthiness, thereby fostering a high level of consumer protection?

### 6.1 The black-box problem & a possible solution

AI-driven smart contracts introduce a new level of complexity by analysing vast amounts of data, identifying behavioural patterns, and adjusting contractual terms and conditions in real-time based on probabilistic reasoning. While their adaptability can offer significant opportunities to enhance consumer protection - by tailoring the contract to better protect the individual consumer they address - it also poses substantial risks, particularly when they fail to operate in a transparent and consumer-friendly manner<sup>133</sup>.

A key aspect in assessing whether AI-driven smart contracts truly foster consumer well-being or undermine it is understanding their decision-making process. Consumers must be placed in a position to *humanly* comprehend the contractual outcomes that involve them. To achieve this objective, it is crucial to neutralise the AI black-box nature, which arises whenever humans cannot clearly figure out the rationale behind AI decisions. Understanding AI reasoning is fundamental to preventing and reacting against biased, unfair, or discriminatory outcomes. Consequently, to mitigate the black-box problem - i.e. the inherent opacity of AI-driven smart contracts - they should incorporate transparency and explainability mechanisms that allow consumers to both understand and, when necessary, challenge AI-generated outcomes<sup>134</sup>. Moreover, AI transparency empowers consumers to be more aware of the consumer-friendly nature of the AI - verifying whether it is operating in a fair and non-exploitative manner - thereby also reinforcing trust in AI-driven transactions.

---

<sup>130</sup> Diogo M Rebelo and Filipa C Ferreira, 'AI-based consumer's creditworthiness assessment: era of automation, future of scoring and the EU policymaking on automated decision-making' [2022] E.Tec Yearbook - Industry 4.0: Legal Challenges 79-81.

<sup>131</sup> See (n 18) 282.

<sup>132</sup> Regarding AI's potential to enhance consumer trust in the e-commerce context and its associated risks, see Minhaz U Akbar, 'The Influence of Artificial Intelligence on Consumer Trust in E-Commerce: Opportunities and Ethical Challenges' (2024) 2(6) European Journal of Theoretical and Applied Sciences 250-257.

<sup>133</sup> Cf. Florian Martin-Bariteau & Marina Pavlović, 'AI and Contract Law' in Florian Martin-Bariteau and Teresa Scassa (eds.), *Artificial Intelligence and the Law in Canada* (LexisNexis 2021) 16-18.

<sup>134</sup> Cf. Karen McGregor Richmond and others, 'Explainable AI and Law: An Evidential Survey' (2024) 3 Digital Society 1, 5-7.



A possible solution lies in Explainable AI (XAI), which shifts the paradigm from an “AI just works this way” approach towards a more consumer-centric model: “here is why AI works this way<sup>135</sup>”. XAI’s potential to generate explanations - using natural language and/or visual representations - can transform the black-box problem in a white-box opportunity by making AI-generated decisions intelligible to the average consumer<sup>136</sup>. Instead of requiring consumers to blindly trust the AI and the trader - who offered the AI-driven transaction - XAI enables interactive engagement with the AI system, allowing consumers to receive clear and human-friendly justifications for contractual decisions.

For instance, in the online retail context, a consumer-centric AI-driven smart contract might detect emotional overspending and compulsive buying patterns, and temporarily block a transaction to protect the consumer from making impulsive financial decisions<sup>137</sup>. In such cases, it should explicitly communicate the rationale behind its action - for example, by informing the consumer that it has identified a spending anomaly based on their behavioural data.

Furthermore, if the consumer seeks a deeper understanding of the AI’s decision-making, they should be able to get to know why and how the AI inferred its conclusion and obtain more information about their behavioural profiling<sup>138</sup>.

Therefore, by integrating XAI mechanisms into AI-driven smart contracts, consumers can gain a clearer understanding of how and why contractual terms and conditions are dynamically tailored to their profile. Consequently, they get the opportunity to assess whether and how these AI-driven tools truly serve their best interests.

In conclusion, this approach promotes a high level of consumer protection by ensuring that AI operates in a fair and transparent manner. With the integration of XAI into smart contracts, consumers are empowered to actively monitor and assess the fairness of AI-driven transactions, ensuring that these tools are genuinely designed in a consumer-centric manner. However, it is not sufficient for AI-driven smart contracts to be merely structured with consumer well-being in mind; consumers must also trust the AI systems<sup>139</sup>. Indeed, trust is a key factor - if consumers do not trust these tools, they will be reluctant

---

<sup>135</sup> XAI aims to produce outputs that are comprehensible to human agents, enabling them to understand why and how an AI system arrived at a specific decision. This transparency is essential to fostering human trust in AI systems, particularly in how they “reason” and “decide”. See Wenli Yang, ‘Survey on Explainable AI: From Approaches, Limitations and Applications Aspects’ (2023) 3 *Human-Centric Intelligent Systems* 162.

<sup>136</sup> Cf. Changdong Chen and others, ‘When Post-Hoc Explanation Knocks: Consumer Responses to Explainable AI Recommendations’ (2024) 59 (3) *Journal of Interactive Marketing* 235-236.

<sup>137</sup> As the AI ultimately drafts the final version of the contract, explains the contractual terms and conditions, and interacts with the consumer to stimulate an economic decision, it behaves as a choice architect that designs the consumer’s choice environment. Consequently, a consumer-centric AI application is required to direct consumers’ attention and actions towards the outcome that best maximises their well-being. Therefore, smart contracts should be developed so that the integrated AI systems are solely capable of nudging consumers with only their interests in mind. Digital nudging should be structured as a tool to enhance consumer economic decision-making, steering them away from decisions that may not align with their long-term goals and financial well-being. Cf. Laurence Devillers and others, ‘AI & Human Values. Inequalities, Biases, Fairness, Nudge, and Feedback Loops’ in Bertrand Braunschweig and Malik Ghallab (eds), *Reflections on Artificial Intelligence for Humanity* (Springer 2021) 80-81.

<sup>138</sup> See (n 1) 113-114.

<sup>139</sup> See (n 132) 255.

to engage with them. As such, it is critical for EU law to explicitly recognise the consumer's right to meaningful, human-friendly explanations regarding AI's decision-making processes, especially when these decisions directly impact their rights and obligations. Ultimately, the right to understand how AI-driven decisions affect them should be recognised as an integral part of consumer rights in the digital era<sup>140</sup>. Ensuring that consumers not only benefit from but also *perceive* the benefit of AI systems will be essential to fostering trust and widespread adoption.

## 6.2 The need for human oversight and intervention

AI-enhanced data processing vastly outperforms human capabilities by analysing large datasets at unprecedented speeds. However, while leveraging this potential can enhance efficiency, it must be accompanied by robust safeguards to mitigate AI-related risks such as biases, unfairness, and discrimination<sup>141</sup>. This is why, to ensure consumer trust in AI-driven smart contracts, a dual approach is required:

1. *Pre-emptive safeguards* to prevent harmful outcomes before contractual decisions are finalised, and
2. *Reactive mechanisms* to rectify unjust decisions after their implementation.

On the pre-emptive side, to prevent biased, unfair, and discriminatory contractual outcomes, human-in-the-loop mechanisms should be embedded within the AI-driven smart contract to enable the human trader to rectify the AI's decisional outcome. Before finalising a contractual decision, consumers should have the opportunity to challenge an AI-generated outcome, prompting human review. If the consumer demonstrates that the AI decision is unjust, the trader should intervene to modify contractual terms and conditions accordingly<sup>142</sup>. This approach offers two important benefits:

1. Consumers can receive fairer contractual terms;
2. Traders can identify and address flaws in the AI system, preventing similar issues from occurring in the future for other consumers.

On the reactive side, if a contractual decision has already been made, human-in-the-loop mechanisms could empower consumers to flag an unjust AI-generated outcome. In such cases, if it is still possible, traders should be required to:

1. Conduct a review to determine whether the AI's reasoning led to an unfair, biased, or discriminatory outcome;
2. Modify the contractual terms and conditions to balance the B2C contractual relationship, if the first assessment is positive;
3. Implement corrective measures to avoid recurring AI errors.

---

<sup>140</sup> Cf. (n 18) 289-290.

<sup>141</sup> Cf. Konstantinos Tsiakas and Dave Murray-Rust, 'Using human-in-the-loop and explainable AI to envisage new future work practices' in Fillia Makedon, *Proceedings of the 15th International Conference on Pervasive Technologies Related to Assistive Environments* (Association for Computing Machinery 2022) 588-589.

<sup>142</sup> Cf. *ibid.* 590-591.



In conclusion, AI-driven smart contracts should incorporate explainability and human oversight as core design principles to balance efficiency with fairness. A legal framework that mandates both transparency and human intervention will enable consumers not only to challenge AI-generated decisions but also to receive meaningful, human-friendly explanations of how and why these decisions were made, thereby preventing AI-driven smart contracts from functioning as opaque and unchecked tools of algorithmic power<sup>143</sup>. Additionally, to foster a high level of consumer protection in the context of AI-driven transactions, EU law should explicitly establish a right to both AI transparency and human oversight. As a result, consumers' trust in these transactional tools could potentially thrive. Ultimately, consumer protection, consumer trust, and AI transparency must go hand in hand to foster a consumer-friendly digital market.

## 7 A possible way forward: the fairness-by-design approach

In May 2022, the European Commission - as part of its Better Regulation agenda, which aims to ensure EU regulations are evidence-based<sup>144</sup> - launched the *Fitness Check of EU consumer law on digital fairness* to determine whether EU laws are adequate to achieve a high level of consumer protection in the digital environment<sup>145</sup>.

The Digital Fairness Fitness Check was published in October 2024 and, among other topics, addressed smart contracts and AI-powered contracting, recognising that they “could increasingly automate all stages of the consumer’s transactional journey” from contract conclusion to its execution<sup>146</sup>. It highlighted risks involving smart contracts - including reduced consumer control and autonomy<sup>147</sup> and challenges in complying with pre-contractual requirements<sup>148</sup>. Additionally, it underscored the threat posed by digital manipulation through dark patterns<sup>149</sup>, manipulative personalisation<sup>150</sup>, and AI

---

<sup>143</sup> As AI-generated decisions may harm consumers - whether through errors, biases, or unfair outcomes - it is essential that both explainability and human intervention are integral to the system’s design. Human oversight is critical at both the preventive and corrective stages. Traders must monitor the performance of AI systems in real-world contractual applications and identify any breaches of consumer law. These may take the form of unfair terms, deceptive commercial practices, misuse of personal data, or manipulative algorithmic techniques. Once such a breach is detected, traders must be able to understand how and why the system produced the unlawful outcome - enabled by integrated XAI mechanisms - and take appropriate corrective actions. Crucially, beyond addressing the specific instance, traders must also ensure that the AI system is subsequently optimised to reduce the likelihood of the same error recurring, thereby fostering a cycle of continuous learning and compliance. Cf. Markus Langer and others, ‘Effective Human Oversight of AI-Based Systems: A Signal Detection Perspective on the Detection of Inaccurate and Unfair Outputs’ (2025) 35 *Minds and Machines* 1, 3-5.

<sup>144</sup> See <[https://commission.europa.eu/law/law-making-process/better-regulation\\_en](https://commission.europa.eu/law/law-making-process/better-regulation_en)> accessed 28 May 2025.

<sup>145</sup> See <[https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/Digital-fairness-fitness-check-on-EU-consumer-law\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/Digital-fairness-fitness-check-on-EU-consumer-law_en)> accessed 28 May 2025.

<sup>146</sup> European Commission, *Digital Fairness Fitness Check* (2024) 82.

<sup>147</sup> *ibid* 195-196.

<sup>148</sup> *ibid* 198-199.

<sup>149</sup> *ibid* 18-20.

<sup>150</sup> *ibid* 30.

applications that exploit consumer vulnerabilities, exacerbating power imbalances between traders and consumers<sup>151</sup>.

To address these challenges, the *fairness-by-design* approach has been proposed as a solution to achieve a high level of consumer protection in digital environments. It entails embedding digital fairness<sup>152</sup> principles into the architecture of AI systems and smart contracts from the ground up, ensuring that they “incorporate consumer protection considerations at all stages<sup>153</sup>” of their development. This strategy establishes consumer protection not as an afterthought but as a foundational design principle. By integrating this approach into the design, development, and implementation of AI-driven smart contracts, it becomes an efficient way to safeguard consumer rights and well-being, while fostering trust and confidence in AI-powered transactions.

Furthermore, adopting the fairness-by-design approach from the early stages of AI and smart contract development aligns with a *positive duty to trade fairly* - an obligation that the Fitness Check proposes to introduce for traders to strengthen consumer protection. Even if this explicit duty is not formally introduced, it could nonetheless be inferred from the professional diligence standard and the general principle of good faith<sup>154</sup>.

Particularly, the fairness-by-design approach could serve as a safeguard, ensuring that AI-driven smart contracts - as a whole and in their components - are designed to comply with EU regulations, detect legal breaches, and prevent consumer harm. One of the most promising applications of AI in smart contracts is its potential to act as a real-time compliance watchdog, monitoring their adherence to EU law. This would shift AI from being a tool of contractual asymmetry to one of consumer empowerment. For instance, if an AI-driven smart contract identifies a potential GDPR violation - such as the processing of consumer data beyond the intended scope - it could automatically halt execution until the issue is resolved, thereby promoting continuous legal compliance monitoring and reducing the risk of regulatory breaches.

Consequently, this approach ensures that AI-driven smart contracts are developed to prevent and mitigate manipulative and exploitative contractual design. To achieve this, the AI system embedded in the smart contract must be capable of probabilistically predicting and detecting potential legal breaches arising from the way it dynamically adjusts contractual terms and conditions. Since these adjustments are tailored to the individual consumer the contract addresses, the AI must be developed to serve and enhance the consumer’s well-being, rather than solely advancing the trader’s interests. Indeed, in line with the obligation of good faith, the AI’s processing of consumer data should not exploit consumer vulnerabilities but instead promote consumer protection.

---

<sup>151</sup> *ibid* 82-83.

<sup>152</sup> *ibid* 1. As explained in the Introduction of the Fitness Check, the concept of “digital fairness” refers to the objective of achieving a high level of consumer protection “in the digital environment, in compliance with the legal standards established in EU consumer law”.

<sup>153</sup> *ibid* 152.

<sup>154</sup> *ibid* 53.



Ultimately, AI's detection and analysis of consumer vulnerabilities - as well as its behavioural profiling processes - must be aimed at protecting the consumer from information, cognitive, and digital asymmetries.

To empower the consumer and address the inherent contractual imbalance in B2C relationships, the AI must shape the contract in a way that:

1. Highlights relevant information to support informed and aware economic decisions - thereby counteracting information asymmetries<sup>155</sup>;
2. Avoids dark patterns and other manipulative designs - thereby protecting consumers from digital manipulation;
3. Safeguards consumers from cognitive biases, heuristics, and emotional responses - thereby preventing the AI from exploiting behavioural patterns.

As a result, the fairness-by-design approach serves as a safeguard to ensure that AI-driven smart contracts are pre-emptively aligned with consumer protection laws, while also enforcing their compliance by designing AI to continuously monitor the contract's adherence to EU law. By requiring AI-powered contracts to be built with fairness-by-design principles, regulatory frameworks ensure that consumer protection considerations are embedded before deployment.

Moreover, this approach offers a balanced regulatory solution by:

- Allowing businesses and AI developers to innovate while ensuring a high level of consumer protection;
- Empowering consumers through AI design that serves and fosters their best interests and well-being;
- Preventing legal conflicts and consumer harm before they arise.

In conclusion, the fairness-by-design approach helps provide a regulatory framework that ensures AI-driven smart contracts remain a tool for consumer well-being rather than a source of new forms of consumer vulnerability. Indeed, embedding the fairness-by-design approach at the core of AI-driven smart contracts ensures that *digital fairness* is not merely a theoretical consumer protection strategy, but elevates itself to a practical safeguard that fosters consumer well-being, without stifling innovation.

## 8 Conclusion

As AI-driven smart contracts become increasingly widespread in B2C digital transactions, it is evident that existing consumer protection laws - designed for traditional, human-negotiated legal agreements - are no longer sufficient. Although an evolutionary interpretation of current regulations may help uphold a high level of consumer protection in the age of AI-powered legal agreements, these frameworks

---

<sup>155</sup> Marcelo Corrales and others, 'Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework' in Marcelo Corrales and others (eds), *Legal Tech, Smart Contracts and Blockchain* (Springer 2019) 198-200.

struggle to address the complexities of automated, self-executing contracts shaped by opaque algorithms and fuelled by behavioural data.

To effectively safeguard consumer rights in this evolving landscape, a modernised, AI-proof legal framework is urgently needed - one that acknowledges the unique risks arising from human-AI contractual interactions and mandates the integration of consumer protection principles into the very design of these technologies.

This paper does not claim to offer an exhaustive analysis. At this early stage in the development and deployment of AI-driven smart contracts, it remains impossible to fully map their capabilities or anticipate the complete range of challenges they may pose. Rather, the primary aim of this research has been to provide a legal reflection on the current and future dynamics between consumers and AI in the context of B2C AI-driven smart contracts, and to propose initial pathways towards a more comprehensive reform.

Emerging as the natural outcome of this legal analysis, the fairness-by-design approach offers a proactive, consumer-centric regulatory model that embeds ethical, transparent, and autonomy-preserving principles into the architecture of AI and smart contracts from the outset. Rather than responding to harm retrospectively, fairness-by-design anticipates vulnerabilities and helps shape digital marketplaces that support rational decision-making, respect consumer dignity, and foster individual well-being.

Ultimately, by anchoring consumer protection in the very code of AI systems, fairness-by-design lays the foundation for a safer, more trustworthy, and human-friendly digital economy.