Digital Vulnerability and the Formulation of Harmonised Rules for Algorithmic Contracts: A Two-Sided Interplay

Teresa Rodríguez de las Heras Ballell

A. Setting the scene and delineating the scope: automated decision-making

Algorithmic and AI-driven automation has pervaded an immense and growing variety of tasks, activities, and decision-making processes in the digital economy. From basic tasks (searching, comparing, ordering, prioritizing, ranking), to more sophisticated added-value services (profiling, personalizing, recommending, multi-attribute rating, filtering, content moderation, algorithmic management, complaint handling, negotiation, automatic adjustment of conditions), they are performed by algorithm/AI-driven systems.

The benefits of efficiency, rapidity, personalization, and cost-reduction have also encouraged the use of algorithmic/AI systems for contractual purposes throughout the entire contract life-cycle: from the negotiation phase to the performance of obligations, termination and enforcement - digital agents; virtual assistants; chatbots; smart products; self-executed smart contracts; personalized transactions; 'dynamic contracts'; automated renegotiation, termination and self-enforcement of agreed consequences for default.

The notion of algorithmic contracting intends to encapsulate all these use cases where algorithmic/AI systems are employed to automate any (one or several) stage/s of the contract life-cycle – from preliminary dealings to termination and enforcement. This intersection between automation and contractual purposes draws the perimeter of the phenomenological scenario for this Paper to test the notion of 'digital vulnerability' and to propose the (sub-)variant of 'algorithmic vulnerability', which is coined, to surface such vulnerabilities specifically stemming from the use of automated decision-making systems (hereinafter, ADM).[1]

[1] ELI *Guiding Principles for Automated Decision-Making in the EU*, at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf.

The premise of this Paper is that the use of ADM for contractual purposes raises issues that trespass and exceed the perimeter of the solutions devised for enabling electronic commerce.

The sentiment that the use of ADM and AI systems in and for contracting implies a new stage in the evolution of contracting forms and contractual practices that goes beyond the challenges of electronic contracting has mobilised not only doctrinal reflection, but also attracted the attention of legislators and regulators on the international scene. The prevailing need to understand the scope of this phenomenon, to assess its implications on existing principles and rules and, where appropriate, to propose specific solutions to mitigate its risks without hindering its penetration in commercial activity or stifling its benefits has prompted study initiatives, proposals for principles and legislative actions in various fora.

The United Nations Commission on International Trade Law (UNCITRAL), whose instruments on electronic commerce have been essential and instrumental in consolidating a body of uniform principles for the first electronic revolution, has embarked, in its Working Group IV on Electronic Commerce[2] , on a project on AI and automation in international trade. In accordance with the mandate received, the group compiled existing provisions in relevant UNCITRAL texts, assessed their suitability for automated contracting and was expected to develop, to the extent necessary, a set of principles[3] and provisions to provide legal certainty for the use of AI systems in the negotiation, conclusion, performance and enforcement of an international contract. At the 57th UNCITRAL Commission session held in New York in July 2024,[4] the work of the WG IV concluded with the adoption of the Model Law on Automated Contracting (hereinafter, MLAC). Thus, UNCITRAL contributes to provide legal certainty for the development and the use of AI to form and perform contracts in international trade.

[2] The author is the Spanish Delegate to the United Nations (UNCITRAL, United Nations Commission on International Trade Law) in Working Group IV. All opinions expressed in this paper are personal to the author.

[3] The current status of the project and session documents are available at https://uncitral.un.org/es/working_groups/4/electronic_commerce.

[4] See https://unis.unvienna.org/unis/pressrels/2024/unisl363.html.

The *European Law Institute* (ELI) issued in 2022 a set of principles for the use of ADM systems[5] (hereinafter ELI *Guiding Principles for ADM*) on which is based the ongoing project on Algorithmic Contracts[6] (hereinafter, ELI *Project on Algorithmic Contracts*) which has started analysing European consumer protection law to assess its adequacy and sufficiency for the use of AI systems in consumer transactions and is in the process of developing a set of principles and model rules for algorithmic contracts with special focus on B2C transactions.

These initiatives are clearly aimed at addressing the legal issues raised by algorithmic contracts with a Private Law approach. But they must also be framed within an expanding universe of norms, recommendations, principles and standards on AI systems that, while not necessarily connected to their use in and for contracting, underpin an increasingly dense regulatory space for the development, implementation and use of AI systems in a socioeconomic context. The AI Regulation (or AI Act) [7] is, in this sense, the most ambitious EU text to lead the building of a regulatory and legislative framework for AI. The AI Act is not designed to govern algorithmic contracts, but it crystalizes several policy decisions and provides for requirements and legal solutions that may transpire increasing global consensus on certain legal standards.

Besides, the AI Act, albeit being the globally recognized landmark of the EU response to AI governance and regulation, it is not in a vacuum and it is accompanied by other important legislative actions aimed at addressing the multifaceted challenges of AI. In fact, the European Union has embarked on an ambitious initiative[8] to review and adapt the regulatory framework

[5] *ELI Guiding Principles for Automated Decision-Making in the EU*, available at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf.

[6] *ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts*, Ongoing Project - https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/.

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), PE/24/2024/REV/1. OJ L, 2024/1689, 12.7.2024.

[8] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe, COM*(2018) 237 final; Commis-

to the digital economy and, in particular but not only, to AI. The two proposals for a Directive on AI liability – Proposal for a Directive on the adaptation of non-contractual civil liability rules to artificial intelligence[9] (AILD) – and for a revision of product liability rules - Proposal for a Directive of the European Parliament and of the Council on liability for defective products[10] (revPLD) - illustrate how this process of modernisation and adaptation has a direct impact on key parts of the private-law system.

The under-construction, changing and still uncertain, above-described legal environment sets the stage for exploring the polyhedric concept of 'digital vulnerability'. As a starting point, the interplay between the rules for algorithmic contracts and the notion of digital vulnerability shows two angles.

Within the scope of the UNCITRAL work, the digital vulnerability does not seem to play a remarkable role, even more, it might be deemed absent in the approach and the deliberations. In consistency with its mandate for harmonizing rules for international trade, acknowledging forms of vulnerability would arguably shift the focus to areas out of the reach of the UNCITRAL's scope. It is not the emergence of vulnerabilities what triggers

sion Staff Working Document, *Liability for emerging digital technologies* - Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, SWD(2018) 137 final; *Ethics Guidelines For Trustworthy AI* from the High-Level Expert Group on Artificial Intelligence, 8.4.2019; White Paper on Artificial Intelligence - *A European approach to excellence and trust, COM(2020) 65* final, Brussels, 19.2.2020; Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Report on the implications of artificial intelligence, the Internet of Things and robotics for security and liability,* COM(2020) 64 final, Brussels, 19.2.2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM(2020) 67 final, Brussels, 19.2.2020. The creation in 2018 of the *Expert Group on Responsibility and New Technologies,* divided into two formations: New Technologies Formation and Product Liability Formation. The New Technologies formation published its report in November 2019 *Report on Liability for Artificial Intelligence and other emerging technologies* (https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en).

[9] COM/2022/496 final.

[10] COM/2022/495 final. P9_TA(2024)0132. European Parliament legislative resolution of 12 March 2024 on the proposal for directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)).

the need for harmonizing rules for the use of AI in international trade, but legal uncertainties and jurisdictional disparities that hamper cross-border transactions. The idea of vulnerability appears, in the international legal harmonization discourse, anchored in consumer-protection considerations that fall outside the remit of 'uniform law for international trade'. To that extent, in the deliberations and in the draft solutions of the UNCITRAL WG IV's work, concerns for digital vulnerability arising from algorithmic contracting is not transpired. In the adopted MLAC, only incidentally in the basic rules of legal recognition or attribution concerns about the vulnerability inherent to the 'automated contracting' may be glimpsed. A specific rule, incorporated as an optional (in brackets) provision, on unexpected actions or decisions of the automated system (Art. 9 MLAC) is probably the only, and most, visible, albeit attenuated by its reinforced optional character for States,[11] permeation of vulnerability considerations in the UNCITRAL text.

Thus, a very dim notion of vulnerability might be glimpsed in the formulation of uniform rules of algorithmic contracting in international trade if it is understood as revealing any situation of asymmetry or inequality in the allocation of risks. From this faded concept of 'vulnerability', it would be possible to affirm that in the formulation of rules that provide certainty, unpredictability, and clear solutions in the attribution of legal effects, the allocation of the risks of errors, unexpected actions, or malfunctioning, or the distribution of liability's consequences, there is actually a perception that the use of ADM (specially, AI-enabled ADM systems) in the contractual process creates new balances or imbalances between the parties that if they remained unresolved or wrongly managed, AI-enabled trade would be disincentivised. It might be argued that uncertainties on the validity and enforceability of AI-performed actions and decisions, the allocation of risks, and the exposure to liability when using ADM systems bring about vulnerabilities that uniform rules aim to prevent or contain. Even at risk of appearing to be a strained interpretation of the notion of vulnerability, it helps to appreciate that the solutions adopted in the formulation of harmonized rules for AI international trade contributes to the discussion and the calibration of digital vulnerability beyond its scope, including in

[11] A/CN.9/LVII/CRP.9 As a model law, States can adopt fully or partially, modify, or not incorporate any provision of the text. Additionally, Article 9 is included in the text in brackets with a footnote advisinfg that "This provision is included for States wishing to enact one or more specific provisions addressin unexpected actions carried out by automated systems".

consumer contracts. Thus, as an illustration, whether the policy decision followed on the allocation of any risks lies in the operator (deployer or user) of the ADM under all circumstances, operators (and, primarily, consumers) are now exposed to a new form of vulnerability that may require a reversal or containment.

Accordingly, regardless of the strong or weak notion of vulnerability that is accepted, the assumption that the basic rules on algorithmic contracting solving the key issues on validity and enforceability, attribution, allocation of risks or liability set the scene where to test and on which to build up a concept of digital vulnerability (narrowed down to 'algorithmic vulnerability') is the backbone of this Paper. Two rules, in particular, are crucial in building a solid framework: legal recognition and attribution (II). Other rules on allocation of errors, or the attribution of unexpected outcomes are also essential and should be studied in depth (but they are not covered in this Paper).

Contrariwise, the ELI project, notably in its first output (ADM-readiness test of EU Consumer acquis),[12] is amply permeated by the acknowledgement that algorithmic contracting (with consumers) creates (or aggravates) new forms of inequality and ADM-specific solutions may be needed for mitigating vulnerability risks. This is the first angle of the interplay between digital vulnerability and algorithmic contracting. A positive correlation that intensifies the vulnerability risk. In this regard, this Paper proposes a narrower notion as a sub-type of digital vulnerability that solely captures the specific challenges stemming from the use of ADM (and not in general from the digital context): it is named 'algorithmic vulnerability'. But the second angle of the interplay between algorithmic contracting and the notion of digital vulnerability provides an inverse perspective. The use of ADM in contracts, specially by consumers, has the potential to revert traditional paradigms, attenuate asymmetries, and repair failures. Consumers might be less vulnerable if assisted by ADM systems. If so, interestingly, new forms of vulnerability emerge when consumers are deprived of the possibility to use such assistive systems, if such a use is prevented, hindered, or rendered unfeasible by traders (by implementing commercial practices, by design of interfaces, or by contractual terms). Hence, countering such

[12] *Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

vulnerability-aggravating situation might require specific provisions aimed at enabling the use, facilitating their operation, and prohibiting (or discouraging) impeding practices, blocking measures, discriminatory terms, or ADM-unfriendly interfaces.

The Paper is structured in four parts including this scene-setting and introductory section. Under this introduction (A), there are two sections, First, section I defines algorithmic contracting, while section II maps the scenarios covered by the notion. The second part (B) identifies and explains the main legal issues arising from algorithmic contracting ranging from the attribution of legal effects to the allocation of liability. This mapping exercise of the main legal issues that algorithmic contracting raises invites the discussion on their interaction with the notion of digital vulnerability. It explores the (two) main legal issues arising from the use of ADM in and for contracting to learn whether it exacerbates, or even have any effect on, vulnerability risks or create new forms of inequality throughout the contract life cycle in commercial transactions. This initial question will be followed by a subsequent one (C) that is focused on consumer contracts to discuss whether consumers are better protected or more vulnerable instead in algorithmic contracts. In examining consumer legislation throughout the lens of algorithmic contracting, some paradigms need to be revisited in the light of new balances and risks triggered by the use of ADM systems in contracting contexts, or at least the rationale behind current safeguards may invite reconsideration. While unveiling and calibrating vulnerability risks raised by algorithmic contracting, it will be discussed whether algorithmic contracting does always and irremediably exacerbate digital vulnerabilities or whether it can reverse or curb this presumed and purportedly inevitable consequence by repairing failures and re-equilibrating asymmetries. If so, which are the sources of these vulnerabilities that are labelled as 'digital' and, therefore, which is or are the triggers. Yet, the next step is to assess whether the existing legal and regulatory framework is suited to prevent these digital vulnerabilities and contain their undesired effects. All these final remarks are summarized in the last part (D).

I. Defining algorithmic contracts

The choice of the term (algorithmic contracts and algorithmic contracting) for the purposes of this Paper is not free of objections and constraints, but there are reasons to endorse its use as reasonable and sufficiently convincing.

'Algorithmic contracting' succeeds in conveying the key elements of the problem to address and in delimiting the contours of the scope. The focus of the Paper is on the use of algorithmic/AI system for contractual purposes at any of the stage of the contract life-cycle. In this regard, the algorithmic/AI system is employed to take a decision or in relation to a decision-making process. Therefore, algorithmic/AI systems, ADM systems, automated systems, and, to a certain extent, automation, and consequently automated contracting and algorithmic contracting, are terms interchangeably used throughout the Paper.

Algorithmic contracting refers to a diversity of phenomenological scenarios where one or both parties use ADM systems (algorithmic/AI systems for decision-making) for purposes related to the negotiation, formation, performance, or enforcement of a contractual agreement. To that end, the term seems appropriate and revealing as it does visibly interconnect the two components of the targeted subject matter.

First, the technological component (automation). It comprises the use of both deterministic algorithmic systems and AI-driven learning systems.[13] The term does not prejudge any technology and, in that regard, it aims to be technology-neutral and model-agnostic. Foundational models[14] are separately defined and subject to specific risk classification and requirements.

[13] Article 2.(1) AI Act:
AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;.

[14] The AI Act does not include a definition of "foundation models" but of "general-purpose AI models" in Article 2(63):
'general-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;.
The seminal report on foundation models proposes a definition based on two key features: i). they are trained on broad data; and ii). they can be adapted to a wide range of downstream tasks. Rishi Bommasani et al. *On the Opportunities and Risks of Foundation Models.* 2022. arXiv: 2108.07258 [cs.LG].

Second, the transactional component (actions and decisions directed to pre-contractual, contractual and post-contractual purposes). The general notion of 'contracting' is intended to cover not only the contract formation stage but any preceding or posterior stage related to a contract or to an envisaged contract. Therefore, this Paper refers to digital assistants searching and selecting best offers for consumers, recommender systems, algorithmic negotiation or renegotiation, AI systems concluding contracts, automated performance of contractual obligations and/or enforcement of agreed consequences in case of default. Thus, algorithmic contracting encompasses pre-contractual actions, contract formation, and a variety of performance-related situations, including termination and enforcement of agreed consequences for default.

The decision to use this term is aligned with the ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts.[15] And it has been employed to define the scope of the ADM-readiness test of the European Union consumer protection acquis conducted as a first result of the Project.[16]

As explained above, the notion of automated system includes deterministic algorithmic models that operate according to instructions and models with AI techniques that incorporate learning capabilities and operate according to (pre-determined or even evolving) objectives. This distinction is particularly relevant for the analysis of vulnerability risks and the assessment exercise on the adequacy of existing legal rules and principles to algorithmic contracts. The most intense impact on the classical elements of private law proves to be particularly exerted by the second category of systems (learning systems). The incorporation of AI techniques provides the distinguishing feature that has, in fact, triggered global concern about its social and ethical implications and has attracted the attention of regulators and legislators worldwide. AI has aroused fear and surprise, scepticism

[15] ELI *Guiding Principles and Model Rules on Algorithmic Contracts,* https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/.

[16] ELI, *Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* adopted by the ELI Council on 27 November 2023. The drafters of the report and co-rapporteurs of the project are Christoph Busch, Teresa Rodríguez de las Heras Ballell, Dariusz Szostek until October 2023, Christian Twigg-Flesner and Marie Jull Sørensen. Available at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf.

and mistrust, fervour and fascination in equal measure. Responses and reactions to and from AI have taken many different forms and formats but share the sentiment of urgency in understanding the risks and the challenges.[17] All of them naturally shape the climate in which legal questions about the use of AI in and for decision-making are addressed.

The formulation of a definition of AI systems for legal purposes faces a number of challenges. It must be free from technological determinants and maintain sufficient (technological) neutrality to encompass the various solutions available (or to come) on the market and to avoid obsolescence by being able to integrate future technological developments. It must translate into functionally and normatively relevant features, operational characteristics and technical specifications. The evolution of the definition of an IA system in the deliberations for an European AI Act[18] highlights these difficulties. The first definition proposed in the AI Act[19] immediately raised several questions and aroused some criticism. Firstly, it failed to convincingly and decisively delineate the proposed AI systems to be regulated from the already commonly used and widely known computer programs

[17] OECD AI Principles, https://oecd.ai/en/ai-principles; Policy paper *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023.* Published 1 November 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023; (European Union) High Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI,* 2019 - https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai -; (United States of America), *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* 30 October 2023 - https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[18] Since the first Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules in the field of artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union, COM/2021/206 final, to the finally adopted AI Act. Throughout the process, the definition has evolved in the successive versions – special reference is made to the version of the text dated 14 July 2023. P9_TA (2023)0236 *Artificial Intelligence Act - Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

[19] The proposed AI Regulation (Art. 3(1)) defined the IA system as
"software that is developed using one or more of the techniques and strategies listed in Annex I and that can, for a given set of human-defined objectives, generate output information such as content, predictions, recommendations or decisions that influence the environments with which it interacts".

(software). The regulatory requirements imposed by the new text required a clear and objective distinction as to their scope of application. Secondly, the reference to certain techniques listed in an Annex, despite the establishment of a review mechanism, questioned (in addition to the uniqueness of the chosen techniques themselves)[20] the technological neutrality, the adaptive capacity to new solutions and the very soundness of a purely descriptive definition incapable of offering a functional concept.

The proposed definition has evolved[21] aligning itself with the OECD notion[22] which, following a subsequent revision,[23] strengthens some of the differential functional features and qualifies others[24] in order to accom-

[20] Proposed AI Regulation, Annex I, Artificial Intelligence Techniques referred to in Article 3, point 1:
"Machine learning strategies, including supervised, unsupervised and reinforcement learning, employing a wide variety of methods, including deep learning. Logic and knowledge-based strategies, especially knowledge representation, inductive (logic) programming, knowledge bases, inference and deduction engines, expert and (symbolic) reasoning systems. Statistical strategies, Bayesian estimation, search methods and optimization."

[21] The latest version of the text, after the compromise agreement reached was made available on 24 January 2024 and includes the following definition: *An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.* In the previous version of the text dated 14 July 2023. P9_TA(2023)0236 *Artificial Intelligence Act - Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))1 defines an "AI system" as *a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.*

[22] OECD, AI terms & concepts, https://oecd.ai/en/ai-principles. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, May 2029.

[23] OECD, AI terms & concepts https://oecd.ai/en/ai-principles, OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, Revision 8 November 2023:
An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

[24] As explained in OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, November 2023.

modate the most recent developments that had burst onto the international scene and media debate (large language models, generative AI, general AI). For the purposes of the AI Act, in order to ensure its coverage in the scope of application and to be able to differentiate, in turn, different regulatory regimes depending on the AI model, in the successive amendments to the proposed IA Act two other definitions were added along with the notion of IA system that were not in the initial version: 'foundation model'[25] and 'general purpose IA system'. Subsequently, in the latest text, these definitions have also changed. Foundation model was finally replaced with 'general-purpose AI model'.

For the purposes of this Paper, the notion of algorithmic contracting starts from the definition of 'AI system' in the European regulation. This is the definition adopted by the final text of the AI Regulation. Four main axes on which the concept of an AI system is based are identifiable: interactivity, adaptivity, autonomy and influence on the environment. AI systems are capable of generating outcomes that influence the environment in which they operate on the basis of a set of objectives, either explicit or implicit, which may have been determined at design[26] or learned later in their operation. These outcomes may consist not only of predictions or recommendations, but also of decisions and content of the most diverse nature. This is widely considered in generative AI models. To generate these

[25] In the text published on 24 of January 2024, the definition of 'general purpose AI model' already is:
an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.
Previously, in the P9_TA(2023)0236 *Artificial Intelligence Act - Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).
Art. 3.1.c) '*foundation model' means an AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks.*
The definition is not included in the latest text after the political agreement in December 2023 and as published in January 2024.

[26] RAJI, Inioluwa Deborah, HOROWITZ, Aaron, KUMAR, Elizabeth and SELBST, Andrew, "The fallacy of AI functionality", *FAccT,* 2022, 959.

results, systems use data or information that they receive, infer, perceive from the environment, and learn by means of learning methods.

The axes along which the definition of AI systems has been built and revolves around are particularly relevant to the legal analysis of automated decision-making and, in particular, algorithmic contracts. There are several very significant implications.

First, the ability of AI systems to perform actions, make decisions and generate content has an immediate, substantial and direct impact on the contractual logic. An AI system can accept an offer, elaborate a contracting proposal, execute an action aimed at fulfilling a contractual obligation, or terminate the contract.

Second, the potential of AI systems to (relatively but increasingly) autonomously learn[27] according to varying levels of autonomy challenges settled notions of consent and intent, error, or actually the conception of contract as a meeting of minds. The very rapid advances of generative AI models[28] and the exponential growth of their capabilities are already beginning to raise the possibility that they may derive in 'emergent behaviours'[29] aimed at circumventing human control, optimising resources to achieve the goal in a sub-optimal way, using persuasion techniques or pretending to be human.

Third, adaptive, learning, and evolving capacity injects unpredictability into the outcome and raises questions concerning the treatment of error, the effect of unexpected or surprising learning, the attribution of legal effects or the allocation of liability.

[27] In this rapidly evolving context, the term 'frontier AI models' has been proposed to define those models with the potential to pose serious risks to public safety and global security. The dangerous capabilities that such AI models would present include even the possibility of circumventing human control through deception and obfuscation. The authors of the paper *Frontier AI regulation: Managing emerging risks to public safety* (2023. arXiv:2307.03718 [cs.CY]) acknowledge that it is not yet clear whether models will tend to develop in this direction, but it is argued that this could be the result of current training paradigms: NGO, Richard,
CHAN, Lawrence and MINDERMANN, Sören, "The alignment problem from a deep learning perspective", 2023. arXiv: 2209.00626 [cs.AI].

[28] OECD, *Initial policy considerations for Generative Artificial Intelligence, OECD Artificial Intelligence Papers,* September 2023, num. 1.

[29] CHAN, A. et al., "Harms from Increasingly Agentic Algorithmic Systems", IEEE Computer Society, 2023, Vol. 2022-March, 2023, https://arxiv.org/abs/2302.10329.

From these defining and differential axes of AI systems, the legal problems of automated contracts emerge, and the legal issues that we are going to analyse are built on them.

From this definition, we can now delineate with full precision the scope and meaning of the notion of algorithmic contracting. Automated contracting comprises the use of AI systems at one or more stages of the life cycle of a contract, by one, several or all parties to a transaction.

Under this broad term, several algorithmic contracting scenarios will be described below with the ultimate aim of assessing the impact on decision-making and gauging the potential vulnerability risks involved therein.

II. Mapping algorithmic contracting scenarios

Firstly, automated systems can be used to exclusively assist a decision or an action finally taken or executed by a natural person or to directly execute the action or take the decision from which the relevant legal effects are to be derived. In the first case, the system selects, compares and recommends the most suitable providers according to certain parameters to facilitate the party's selection and final decision process. In the second scenario, the system repeatedly and automatically, without human intervention in each of the actions, assesses the suppliers, reviews the conditions and continuously concludes supply contracts to optimise the value chain. The legal issues are more numerous and substantial in the second scenario.

Secondly, automated systems can be used exclusively by one of the parties or by several or all the parties involved. Considering the negotiation, conclusion or performance of a bilateral contract, the unilateral use of an ADM system by only one of the parties will raise issues arising from human-machine interaction such as the need to disclose that an ADM system is used, the actual freedom to decide whether or not to contract with or restrict the use of automated systems, the ability of the system to process all information generated in the interaction (the requirement for terms and conditions to be in an accessible and machine-readable format)[30] or, for example, the risk of manipulation of the ADM system. The dual (or

[30] Article 14 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act, hereinafter DSA), OJEU No. 277, 27 October 2022. DUCATO, Rossana and STROWEL, Alain, 'Limitations to text and data mining and consumer empowerment: making a case for a right to machine

multilateral, if relevant) use of ADM systems leads to an environment of pure and full interaction between 'machines' (M2M, *Machine-to-Machine*) where in addition to all the general issues (validity, attribution, liability, pre-contractual information) it could suggest new ones such as the effects on the contract of interoperability restrictions, the reconsideration of the notion of balance or imbalance in the negotiating position of the parties or, if the parties use a common platform for their interaction, the risk of conflicts of interest or the intervention of the platform operator as an intermediary (mediator, service provider, representative, agent).

ADM systems can be used in consumer relations, either by the consumer (virtual assistants,[31] *chatbots*, digital assistants)[32] or by the trader, or by both parties. The impact of the use of ADM systems in consumer relations,[33] especially when it is the consumer who uses them, goes beyond mere questions of terminology and the applicability of consumer protection legislation to these cases, and may invite a profound and radical rethinking of some of the paradigms that have established the foundations on which consumer law has been built.

legibility', *International Review of Intellectual Property and Competition Law,* 2019, vol. 50, num. 6, 649-684.

[31] To the extent that a virtual assistant, as defined in the EU regulation, performs an action with contractual effects, e.g. initiating a subscription or executing a contractual obligation or right (such as access to a service). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Regulation). OJEU No. 265 of 12 October 2022 (hereinafter the GDPR).

Art. 2.12). "*Virtual assistant" means software that can process requests, tasks or questions, including those formulated by means of sounds, images, text, gestures or movements and that, on the basis of such requests, tasks or questions, provides access to other services or controls connected physical devices.*

[32] Or *intelligent agents* in the sense of Arno R. LODDER and Marten B. VOULON, in "Intelligent Agents and the Information Requirements of the Directives on Distance Selling and E-commerce", *International Review of Law, Computers & Technology,* 2002, vol. 16, 77.

[33] SEIN, Karin, "Concluding Consumer Contracts via Smart Assistants: Mission Impossible under European Consumer Law", *Journal of European Consumer and Market Law,* vol. 7, 2018, 179; BUSCH, Christoph, "Does the Amazon Dash Button Violate EU Consumer Law? Balancing Consumer Protection and Technological Innovation in the Internet of Things", *Journal of European Consumer and Market Law,* 2018, vol. 7, 80.

On the one hand, the *acquis communautaire* on consumer protection seems to respond to the use of automated systems (*ADM-readiness test*)[34] with consistency and, upon implementing certain improvements and modifications, it seems to maintain robustness and effectiveness. However, this conclusion of reasonable adequacy does not necessarily imply that 'no action' is the optimal strategy or the one that guarantees resilience and sustainability in the future. For, in fact, on the other hand, far-reaching movements are transpiring in the conception of the underlying asymmetry in the consumer relationship that may require rethinking some of the paradigms of consumer law. While the intensive use of AI seems to aggravate the exposure to vulnerability risks, making vulnerability (digital vulnerability)[35] almost endemic in the digital environment, it heralds, on the other hand, an empowerment of the consumer that strengthens their bargaining position and would seem to question the value and ultimate function of classic protection measures such as information rights. It may be argued that an 'augmented consumer', assisted by automated systems in making much more 'informed' decisions, is emerging. This is a critical turning point where risks and vulnerabilities are magnified, while at the same time, the asymmetry of the bargaining process might be substantially reduced and some of the classic protective responses to consumer relations might start losing, in this context, their meaning and purpose, at least to a certain extent.

Thirdly, in automated (or algorithmic) contracting, a distinction has to be made between the contract in relation to which the AI system is used in one of the contractual steps and the peripheral contracts necessary for the use of such an ADM system for the negotiating purpose. Contracts for the supply of ADM systems, for the design or development of an AI system, for training, for the provision of data or for upgrades necessary to be able to negotiate, conclude or execute an algorithmic contract define the ecosystem

[34] This is the main, and provisional, conclusion of the report produced by the team of the *ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts*, after conducting the *ADM-readiness test* on the main consumer rules of the *acquis communautaire*. ELI, *Interim Report*, *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* adopted by the ELI Council on 27 November 2023. The drafters of the report and co-rapporteurs of the project are Christoph Busch, Teresa Rodríguez de las Heras Ballell, Dariusz Szostek until October 2023, Christian Twigg-Flesner and Marie Jull Sørensen.

[35] HELBERGER, N., SAX, M., STRYCHARZ, J., MICKLITZ, H.W., "Choice Architectures in the Digital Economy: Towards a new understanding of digital vulnerability", *Journal of Consumer Policy*, 2022, vol. 45, 175-200.

necessary for algorithmic contracting to take place. The focus is not on these agreements, which may or may not be partially automated, but on the final contract that is negotiated, concluded or executed using AI systems whose availability depends, in effect, on this prior or contemporaneous contractual framework. The contract we are interested in is not the one concluded between the party who wants to use an AI system to negotiate with his suppliers and the developer of such a system, whether standard or customised. However, in the analysis of some of the issues that should be addressed, this interaction and influence may be relevant. Thus, for example, knowing the conditions under which the design and development of the AI system has been commissioned may be a factor in assessing the degree of control of the system by the operator using it in automated contracting, in assessing the existing of an error, or in choosing product liability rules as a response to an unforeseen action of the system causing damage

B. Identifying legal issues of algorithmic contracts and exploring uniform solutions

Electronic contracting, a few decades ago, posed a challenge to legacy contract law.[36] Traditional contract-law rules had been ideated, formulated, and applied, paradigmatically, for face-to-face and in-writing distance transactions highly dependent upon the available medium, dominantly paper, and the means of communications for sending and received relevant declarations and other statements between the parties. The use of telephone or telegram had indeed required, prior to the advent of digital technologies, an explicit legal recognition in civil and commercial codes. Electronic contracting confronted traditional contract law with the admissibility of the digital medium as a functional equivalent to writing in paper and the use of electronic communications[37] to express and convey declarations of

[36] UNCITRAL texts in the 1996 Electronic Commerce Model Law (with Guide to Enactment) – hereinafter, MLEC; 2001 Electronic Signatures Model Law (hereinafter, MLES); 2005 Use of Electronic Communications in International Commerce Convention (hereinafter, CEC) approved by General Assembly Resolution 60/21, of 23 November 2005.

[37] CEC Article 8. Legal recognition of electronic communications

will and other statements with pre-contractual, contractual or contract-performance relevance. Under the fundamental principles of technology neutrality and functional equivalence, essentially, [38] international instruments and domestic legislation incorporated the necessary provisions to ensure the validity and enforceability of electronic contracts[39] as well as other declarations or actions along the contract life cycle.

Algorithmic contracting, as defined above, goes beyond electronic commerce and pose additional challenges to existing legal rules, even if they are modernized to accommodate electronic contracts. While electronic commerce's challenge stems from the use of electronic communications, algorithmic contracting's one lies in automation.

ADM systems do not simply transmit or enable the transmission of an offer, an acceptance or any other relevant communication between the parties as electronic means do, but, in assisting, or even making decisions, they (automatedly and autonomously, that is the key) produce an output, that may amount to be an offer, an acceptance, or a communication of contractual modification.[40] The difference is substantial and enormous. The simple problem of attribution that electronic communications, once their

"1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.
(…)"
"Electronic communication" is defined as "any communication that the parties make by means of data messages; while "data message" is defined as "information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy".

[38] Mainly, as formulated in MLEC, MLES, and CEC.

[39] Article 12 CEC seems to go further than the pure electronic contracts and explicitly acknowledges:
"A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract."

[40] As an illustration in the EU *acquis*, Article 9 of the Directive on Electronic Commerce (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ L 178, 17.7.2000, 1–16) does not refer to contracts concluded by automated means, but simply to contracts concluded by electronic means:
Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic

validity and enforceability had been recognised, posed, and was effectively solved, is exacerbated by automation. If ADM systems repeatedly and automatedly (even more intensively if autonomously) produce outputs, without human intervention in each and every action and decision, the question of to whom to attribute such decisions and their resultant legal effects is of paramount importance. The answer is neither evident nor necessarily easy. As automation includes not only deterministic algorithmic decision-making but also AI-driven learning systems, the attribution of legal effects and the allocation of risk in case of mistakes, damages or harmful consequences gain complexity and significance. To the automated self-execution, it has to be added the assumption of certain levels of autonomy in the decision-making and the performance.

Therefore, it has to be discussed whether existing legal rules on electronic contracts are suited to algorithmic contracting on an extended functional-equivalence approach, or, on the contrary, there are novel challenges that algorithmic contracting poses.

Algorithmic contracts tense the most classical features of the notion of a contract as a meeting of minds. Unlike electronic contracts that simply transform how declarations of wills are manifested, stored, and transmitted, algorithmic contracting touches the human-centric core of contract law. Although humans are not certainly excluded from the scene, as they participate in designing or deploying the system, they may express their consent in using such automated mechanisms for a particular purpose (or the consent might be inferred from the fact of deploying and using), or they (can) select the criteria on which the system operates, or the data sources feeding the ADM system, the distinctive features of ADM precisely lie in the decision-making capabilities of the system and its operation "without human intervention" in each and every action carried out thereby.

Therefore, the validity and enforceability of contracts concluded by ADM as well as of any action performed in connection with any stage of the contract life cycle (pre-contractual, contractual, performance, termination) need to be assured.

contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

The current wording acknowledges two fundamental principles: first, that contracts can be validly negotiated and concluded by electronic communications: declarations (data messages) in digital form and transmitted by electronic means; and secondly, that contracts can be validly concluded in a digital medium.

I. A rule of legal recognition

A strong case is made to unambiguously harmonized a rule of legal recognition.[41] Such a rule must recognize that the validity and enforceability of a contract should not be denied on the sole ground that it is was formed by automated systems. This rule entails that other grounds could challenge the validity or the enforceability of the contract though ("on the sole ground that"). The fact that automated systems have, without human intervention, formed the contract is not compromising the validity or enforceability of the contract. Additional rules may be required (and should be indeed formulated) to address other issues that are likely to impact on the validity and enforceability of the contract, such as the state of mind, mistake, or any other defects of consent. Nevertheless, a firm legal recognition as formulated above is instrumental to lay the foundations to establish a sound legal framework for algorithmic contracts. It dissipates any fundamental and radical objection in admitting that they can be legally binding contracts despite the 'human distance' from the processing to reach a meeting of minds.

No distinction, at least in principle, should be drawn between dual situations where both parties are automated systems or non-dual ones if only one of the parties is resorting to an automated system. As far as the legal recognition principle is concerned, there is no solid reason to alter it. However, specific rules or safeguards might be necessary in the second

[41] UNCITRAL, A/CN.9/WG.IV/WP.182, 4:
Principle 2. Legal recognition
(a) A contract is not to be denied validity or enforceability on the sole ground that an automated system was used in its formation.
(b) An action in connection with the formation of a contract is not to be denied validity or enforceability on the sole ground that it was carried out by an automated system.
(c) An action in connection with the performance of a contract is not to be denied validity or enforceability on the sole ground that it was carried out by an automated system.
In the final version of the MLAC (A/CN.9/LVII/CRP.9), the rule of legal recognition is laid down in Article 5:
Article 5. Legal recognition of automated contracting
1. A contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in any action carried out in connection with the formation of the contract.1
2. An action carried out by an automated system in connection with the formation or performance of a contract shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed or intervened in the action.

scenario if a special vulnerability arising from human-machine interaction is assumed and expected to be mitigated.

The rule of legal recognition is to be extended over any action in connection with the contract and throughout the entire contract life cycle. Thus, it includes actions carried out by the automated system during the precontractual stage (automated negotiations), a unilateral proposal to renegotiate a formed contract, actions to perform by one or both parties any of the contractual obligations, an action to exercise a right to withdrawal, or a prior notice for termination.

The term 'action' is intendedly neutral and aims to encompass all kinds of outcomes an automated system may generate. These outcomes, in the context of a commercial transaction, range from mere mechanical actions activated by the instruction sent by the ADM system to the interconnected device, to content generated by the system and addressed to a variety of recipients (humans or devices) – data, code, digital content, digital service – to be processed. Hence, the outcome can consist of an instruction sent by the ADM system to a delivery robot to process a purchase order, a specific data to be integrated in the contract (an update of the rent or the price fixed as per the pricing mechanism), or a draft document (an offer, a draft contract, a legal brief, a notification as per the contract, a termination letter) or any other content (voice, visual art, music or code). As foundation models and generative-AI tools are gaining overwhelming scale and growing sophistication, generative capabilities have to be properly acknowledged and sufficiently embraced by any terminology employed to describe which actions are carried out by automated systems.

The choice of a perfect term to embrace all these types of outcomes automated systems are capable of generating is not easy.[42] 'Actions' seem a viable solution to the extent that cover equally a variety of outcomes that may have legal effects and, therefore, will be subject to a proper legal categorization in each case. The idea of using explicitly the term 'decisions' to classify certain outputs generated by automated system raise concerns about an attempt to attribute legal capacity and personify automated systems. To avoid such a misconception, it seems more reasonable to keep the notion neutral and address the attribution issue with an attribution rule, as discussed below.

[42] UNCITRAL, A/CN.9/1132, para. 65(b)) Deliberations of the Working Group IV on this matter (see A/CN.9/1125, paras. 28, 69, 77 and 86; A/CN.9/1093, para. 56).

II. Attribution rules

The legal recognition rule leads to a fundamental discussion on attribution of the legal effects. Having discarded any attempt to grant personhood or recognise automated systems as distinct and separate persons, an attribution mechanism is essential. Promoting algorithmic contracting in and for commercial activities depends upon a predictable and sound enabling legal framework providing clear rules for attribution of legal effects, and allocation of risks.

Several features of algorithmic contracting explain why attribution may be uncertain.

First, AI system can operate with 'varying levels of autonomy'. Assuming certain levels of autonomy and learning capabilities of the AI system questions a perfect, deterministic predictability of the output and, therefore, challenges a simple attribution model. How to face unexpected outputs from the perspective of contract rules?

Second, various actors are involved in the design, the training, the deployment, and the operation of an ADM system. Hence, it can be discussed whether the outputs are decisively, majorly, or partially determined by the design, by the completeness and adequacy of the training process, by the quality and the quantity of data, by the decision to use that system for a particular purpose, or by the lack of an update. All these elements can influence on the final output, but it has to be decided to whom to attribute the output and its legal effects. This question is not referring to the allocation of risks and, therefore, it is not diving into the liability rules. The attribution question is simple, but essential. Whose actions are carried out by the system? Should the output generated by the ADM system turn out to be an offer, who is the offeror; should the system accept an offer and the contract is concluded, who are the contracting parties; should the system omit relevant information in the negotiations, who might be held liable for infringing the pre-contractual duty to inform; should the system send a notice of termination, whether the contracting party is duly exercising their right to terminate with prior notice.

Third, complexity, opacity, data-dependency or openness characterizing AI systems may obscure a full and total comprehension of the process leading to the output to be attributed, even by the person who uses the system for a particular purpose. A company who relies on an automated-negotiating solution may feel that the preliminary dealings are developing in an uncontrolled or unexpected manner, or simple that they are inexplicable.

These features characterising AI-driven decision-making lead to two undesired risks.

On the one hand, uncertainties on the attribution of the outputs and their legal effects. Contracting would be highly discouraged, if parties are uncertain about who is engaged in the negotiations and who is the counterparty. Such an ambiguity is simply an unacceptable risk for the commercial activity. It would be unexpected for a negotiating party to realize that the binding offer produced by an automated negotiating system is surprisingly attributed to the programmer of the automated system, unknow by the party and unconnected to the negotiations, a data provider, an update provider or any other actors involved in the design, the deployment of the training of the automated system. That is an absurd and surprising result. It has to be prevented with the formulation of a clear attribution rule. In the dim notion of vulnerability that was used at the beginning, it can be argued that the characteristics of AI may create situations of asymmetries, imbalances, and uncertainties throughout the contract lifecycle that require a proper adjustment. To that extent, it was suggested that vulnerability can also be combatted with the formulation of (harmonized) basic contract rules aimed at clarifying attribution, ensuring predictability in the allocation of risks, or providing clear rules on error, unexpected outputs, or malfunctioning.

On the other hand, parties might opportunistically allege such features of AI system (complexity, opacity, vulnerability, data-dependence or openness) as an excuse not to assume the consequences of such actions or not to comply with their obligations. Parties engaged in algorithmic contracting might be tempted to avoid their obligations on the grounds that the relevant actions were carried out by automated systems. This risk would destroy legal certainty in trade and definitively ruin the prosperity of algorithmic contracting. In the same vein, not addressing this opportunistic risk with adequate rules would stoke forms of vulnerability on the counterparties.

A simplified attribution rule that states that the actions of a system shall be attributed to 'the person on whose behalf the system is operated'[43] has several serious limitations.

First, it is only providing a solution when that person on whose behalf the system is operating can be identified. The difficult cases are where such a link is not explicit or evident and cannot be inferred from the circumstances. Two illustrations can help to distinguish such cases. If the

[43] UNCITRAL, A/CN.9/WG.IV/WP.182, Principle 4.

chatbot engaged in the negotiations is embedded in a digital environment (website, platform, app) visibly controlled and managed by a company (the trader), these circumstances lead to presume that the chatbot's actions are attributed to that company. If the parties agree to use automated systems to fix certain criteria for the performance of their contractual obligations, such an explicit identification is sufficient and conclusive. Complications arise from cases where neither the parties state, nor the practices between the parties or the surrounding circumstances reveal such an assumption.

Second, the relationship between the ADM system and the person to whom to attribute its actions is not and should not be treated as an agency relationship. The automated system is not 'acting on behalf of' in pure terms ('the person on whose behalf the system operates'), as that might re-open the debate on the personhood of AI systems. Should the wording 'on whose behalf the system is operated' is, however, simply referring to the fact that the system is operated (by a third party) on behalf of the principal (to whom to attribute), this is not more than a traditional rule of attribution between persons (agent and principle). If it is formulated so, there is no mystery. The real conundrum is to whom to attribute the actions of 'the' system as such.

Third, the attribution rule should not only provide a predictable and objective model for third parties interacting with the automated system to rely on, but also for the person to whom the actions are to be attributed. Such an attribution should not be unexpected, unreasonable or surprising when based on or dependent upon inadequate factors to presume attribution. In this regard, the mere use, as a pure factual factor, might be inadequate. Some illustrations may explain better the inadequacy. A bank decides to use a chatbot to handle complaints from its customers, and unexpectedly the chatbot renegotiates the loan conditions. An industrial company uses robots in its smart warehouse, and in one of the updates entirely conducted and controlled by the manufacturer, a smart functionality is installed in the robots that become to make purchase orders on an automated basis. A new office building is equipped with sophisticated smart devices and systems collecting data from staff performing and a business rent the office space without predetermining which data will feed the systems and on which criteria operate, but the automated gates start banning the entry to employees classified, by the system, as 'unreliable'.

Considering the unwanted effects of the 'use' as the single factor for attribution, two other elements can be considered: control and purpose.

The (natural or legal) person who decides to use an automated system for contractual purposes is expected to adopt measures to keep it under certain control: commissioning the design of the system under a set of instructions, customizing a standard system provided in the market by a developer, fine-tuning a general-purpose model, ensuring that it is fit-for-purpose, seeing to timely maintenance or update, or deploying a proportionate human supervision. It cannot be ignored that the concept of control is elusive and complex, and maybe it should be labelled differently to avoid confusion with the notion of 'control' enshrined in other UNCITRAL instruments (notably but not exclusively, the Model Law on Electronic Transferable Records, MLETR)[44]. Specially, control potentiality seems to contradict the characteristics inherent to AI systems (opacity, complexity, autonomy, openness). Nevertheless, the idea of control is still the most convincing to bridge the attribution link, albeit embedded in other elements. The control factor is not aimed to be used as a limitation or an excuse for a party to assume its actions in a contractual context, by proving lack of control; on the contrary, the notion of control intends to find a reasonable solution where parties are silent, as well as to provide incentives for the parties using automated systems to adopt proper measures to effectively take control.

In the final text, the MLAC tackles the attribution problem with a two-layer rule (Art. 7 MLAC). First, in concordance with primary B2B scope, parties' autonomy. Paragraph 1 states: 'As between the parties to a contract, an action carried out by an automated system is attributed in accordance with a procedure agreed to by the parties'. Second, a combination of 'use' and 'purpose'. Thus, if paragraph 1 does not apply, 'an action carried out by an automated system is attributed to the person who uses the system for that purpose'.

The presumption of attribution by a qualified use (not a passive use but an active use based on the capacity of influencing to some extent on determining performance criteria) would also apply to a consumer who uses an ADM system in or for contracting purposes (digital assistant). In this case, however, additional safeguards might be required. In the ELI Project on Algorithmic Contracts, several solutions have been proposed.[45]

[44] UNCITRAL Model Law on Electronic Transferable Records, 2017, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records.

[45] ELI, *Interim Report*, *EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?,* adopted by the ELI Council on 27 November 2023. The drafters of the report and co-rapporteurs of the project are Christoph

First, that the ‘control’ by the consumer in the terms and to the extent set out below should be configured as a design parameter (*control by design*).

Second, that ADM systems for offering virtual assistant services to consumers that allow automating any of their stages of the contract life cycle should be classified as high-risk systems, in the classification of the AI Act.

Third, that consumer’s ‘control’ should be understood to exist only if the following three requirements are satisfied: a). the ability to approve or object to a contract agreed through a digital assistant prior to its conclusion; b). the ability to set (and review) the parameters that a digital assistant uses to make its decisions; c). the right to suspend or disconnect a digital assistant. In the latter case, the exact scope of this right could depend on the types of business models, or monetisation strategies, that may emerge in relation to digital assistants, in particular where these are an integrated feature of physical products (*smart products*).

The approach adopted by the ELI Project invites two deeper reflections.

On the one hand, if and to which extent the attribution phase and the selected attribution factors (may) constitute a potential source of digital vulnerability in consumer transactions. Should the attribution factors fail to effectively and properly articulate the actual consent of the consumer and convey in an equivalent way an informed decision, the consumer is exposed to new forms of vulnerability. Then, it should be asked whether a specific action is needed to alleviate such a risk.

On the other hand, if the attribution solution formulated as a harmonized rule in the UNCITRAL work has not been, in principle, guided by any vulnerability concern, whether the same attribution factors can and should work in a different scenario intersected by the perception of higher vulnerability risks. The question is fascinating as it leads to a profound and radical discussion on policy options. Should attribution be indeed a common issue, regardless of the condition of the parties, the rule and the factors should remain intact. How then to protect vulnerable parties at this stage? One option is to accommodate the attribution rule or the attribution factors in order to prevent vulnerability scenarios. That raises the delicate issue of the reasons to differentiate basic contract-law rules depending on the condition of the parties, or maybe the circumstances of the transaction (environment, means, interfaces). The latter one addresses an interesting structural perspective of the digital vulnerability – linked to and stemming

Busch, Teresa Rodríguez de las Heras Ballell, Dariusz Szostek until October 2023, Christian Twigg-Flesner and Marie Jull Sørensen.

from the environment itself. Another option is not to alter the basic rule of attribution, but to work on defining specific and more adequate control criteria, together with other safeguards (right to object), to prove relevant control for attribution purposes.

The discussion above bridges the formulation of harmonized rules for the use of AI/ADM systems for contracting purposes with the debate on digital vulnerability in the context (consumer) algorithmic contracting.

C. Decoding digital vulnerability in algorithmic contracting: a two-sided interplay

A digital-vulnerability approach to algorithmic contracting leads, at least in an initial phase, to consequently advocate for the preservation of the paradigms and the backbone principles of consumer protection legislation. That would result from three main principles: the principle of attribution, the principle of application of consumer rules, and the principle of non-alteration of the duty to provide information. As per the principle of attribution, the starting point is that the actions and decisions of the virtual assistant are 'of the consumer'. That is, properly coupled with design measures that ensure that the consumer has and retains control, the actions of the ADM system are considered by the law as actions attributable to the consumer. Thus, the status of the parties (consumer-trader) is not altered by the use of ADM systems. The immediate and natural consequence is therefore the principle of application of consumer law, as the conditions for its application would not have changed in any way. In particular, the information obligations, which channel the paradigm of transparency in the consumer market, should not be reduced or altered despite the intervention of virtual assistants.

With the above three principles, algorithmic contracting in consumer relations is based on the logic and principles of consumer protection law. Notwithstanding this at least provisional conclusion, the opportunity should not be missed to reopen certain debates and to question some of the solutions embedded in the current conception of consumer law. It is an old debate that warns that information obligations are, on the one hand, a burden[46] for the trader, heavier as smaller is the size, and, on the other

[46] BEN-SHAHAR, Omri and SCHNEIDER, Carl E., *More than you wanted to know: The failure of mandated disclosure. Princeton,* NJ: Princeton University Press, 2014;

hand, that they are very often (at least to some extent) inefficient[47] and do not produce the expected result. The information model has obvious limits that blur its effectiveness. Limitations in information processing or comprehension, short attention spans, lack of reading, imperfect rationality, cognitive biases and prejudices, education and experience, are factors that inevitably impact on the foundations of the model.[48] Flooding the market with information does not lead to the myth of perfect transparency, nor does it necessarily lead the normative consumer model to make rational, pro-consumer decisions. While information obligations continue to increase in legislation and, in particular in relation to AI systems, continue to play a protective role, there is a call for a transformation of information duties,[49] an adaptation of the form, channels and characteristics of the message to ensure its readability, comprehensibility, appropriateness and adequacy, personalisation and contextualisation. Digital assistants and other AI systems could be designed to meet these expectations by improving the comprehensibility, contextualisation and sufficiency of information, adjusting its tone and personalising the content, completing, verifying or expanding where necessary for each consumer and each transaction. But, we may ask ourselves, does this make the consumer more powerful or does

GARCIA PORRAS, Catherine and VAN BOOM, Willem, "Information disclosure in the EU Consumer Credit Directive: Opportunities and limitations", in J. DEVENNEY and M. KENNY (eds.), *Consumer credit, debt, and investment in Europe*, Cambridge, UK: Cambridge University Press, 21-55; MAROTTA-WURGLER, Florencia, "Will increased disclosure help? Evaluating the
recommendations of the ALI's 'principles of the law of software contracts", *University of Chicago Law Review*, num. 78, 2011, 165-186; MAROTTA-WURGLER, Florence, "Does contract disclosure matter?", *Journal of Institutional and Theoretical Economics*, num. 168, 2012, 94-119.

[47] SEIZOV, Ognyan, WULF, Alexander J. and LUZAK, Joanna Aleksandra, "The Transparent Trap. Analyzing Transparency in Information Obligations from a Multidisciplinary Empirical Perspective", *Journal of Consumer Policy*, num. 42, issue 1, 2019, 149-173.

[48] BAR-GILL, Oren, "Consumer Transactions" in ZAMIR, Eyal and TEICHMAN, Doron (eds.), *The Oxford Handbook on Behavioural Economics and the Law,* Oxford: OUP, 2014, 465-490. AYRES, Ian, and SCHWARTZ, Alan, "The No-Reading Problem in Consumer Contract Law", *Stanford Law Review*, 2015, vol. 661, 545-610.

[49] PICHONNAZ, Pascal, "Informed Consumer or Informed Parties: Towards a General Information Duty?", *European Journal of Consumer Law/ Revue européenne de droit de la consommation* (EJCL/REDC) 2023/2, *Is consumer law obsolete?*, 267-281; PICHONNAZ, Pascal, "The transformation of information duties", in TWIGG-FLESNER, Christian and MICKLITZ, Hans (eds.), *The Transformation of Consumer Law and Policy in Europe,* Oxford/London: Hart/Bloomsbury, 2023.

it make him responsible for his own protection? Does it make sense to shift the burden of the information duty from the trader to the consumer assisted by AI systems? What effects would this shift have on the market in general and on the liability of traders in particular?

The starting point here should be then the opposite: the use of ADM systems for consumer decision-making can strengthen the consumer's position and improve bargaining power. If a consumer, assisted by a digital assistant, i.e. by an AI system that searches and processes information, selects and recommends options or even makes the final contracting decision with a prior review of the purchase conditions, is in a position to make better informed decisions, the use of ADM systems in consumer relations accompanies and makes the protective function of consumer law more effective. If such a premise is assumed, the limitation or prohibition of their use will be avoided or prevented as far as possible because it empowers the consumer. The underlying debate is much more complex, with more nuanced premises and less forceful conclusions, but at this point we only take one of the argumentative threads to address the question of the conventional prohibition of the use of automated systems, in particular by the consumer. In short, whether the principle of non-discrimination of ADM systems in contracting, reinforced by the premise that it also mitigates the consumer's vulnerabilities and improves his bargaining position, is transformed into a right of use without limitations or barriers in consumer relations. Interestingly, this idea shifts the spotlight from the assumption that ADM systems generate new forms of vulnerability to the enticing presumption that a consumer deprived of the assistance use of ADM is rendered more vulnerable. Accordingly, vulnerability faces must be also attacked by ensuring fair access and equal use to those systems likely to reinforce the consumer position in contracting.

Without going into the body of the study, which deserves due attention elsewhere, we dwell on one of the principles proposed in the ELI (*European Law Institute*) project on algorithmic contracting.[50] Of the eight principles

[50] Details of the ongoing *ELI Project on Guiding Principles and Model Rules on Algorithmic Contracts can be* found at https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/. The report approved by the ELI Council on 27 November 2023 and published in the same year, *Interim Report, EU Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM,* examines the adequacy of existing rules while already anticipating some of the principles that will guide the second phase of the project aimed at formulating a set of principles and model rules for automated contracting.

tentatively proposed in the first phase of the project, principle 4 (*Non-discrimination and 'no-barrier' principle*) encapsulates the idea that consumers can benefit from the use of ADM systems for trading and contracting. Moreover, ADM systems in the form of digital or virtual assistants can most effectively and fully realise the ultimate ratio of the 'informed decision'[51] which the consumer makes with full knowledge and full, adequate and sufficient information to ensure that it is in his or her best interests. Both in their current state of development and in their expected future evolution, ADM systems operating as digital or virtual assistants for consumers would act as powerful managers of transaction-relevant information. They can collect, contrast, compare and verify information provided by traders about the product, recommend the best combination of attributes, advise on the most appropriate contractual terms, negotiate certain terms, search for the best offer, reject proposals incorporating contractual terms that the consumer has marked as unacceptable, or dynamically review long-term relationships such as subscriptions or contracts for the supply of products or services. These functionalities and potential applications of digital assistants would seem to dilute the weakened position of a consumer unable to deal with scattered, overwhelming, biased or complex information. The digital assistant stands as a consumer protection wall and a 'manager of consumer interests' with unparalleled collection, verification, integration and search capabilities.

On a first reading, algorithmic contracting would seem to rebalance consumer relations, eliminating asymmetries and reducing the need for safeguards. But the context is much broader and more complex and cannot, and should not, be solved with the erroneous assumption that there are no more 'consumer relations'. Indeed, as a starting point, the ELI project on algorithmic contracting starts from the principle (*Principle 2: Application of Consumer Law to Algorithmic Contracts*) that the actions of the virtual assistant are attributed to the consumer and, as such, we are dealing with consumer relations to which consumer protection rules apply. Perhaps this should only be an interim and transitory answer that will have to be discarded when (if) the transition to M2M transactions in all economic

[51] Article 2(e), Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council. (*Unfair Commercial Practices Directive*), OJEU L 149/22, 11.6.2005.

operations is completed. Then, we will have to refocus intervention on 'technological asymmetries' and 'digital vulnerabilities'.

Nor are we here analysing the intricate question of the attribution of information from the virtual assistant to the consumer and its possible impact on the content and scope of the information obligations of the trader.

Therefore, we are only assessing whether, given the effect of the strengthening of the consumer's position that the use of automated systems seems to have, the limitation or prohibition of their use by the employer would be appropriate. The principle of non-discrimination and *non-barrier* has two derivatives. On the one hand, the prohibition of a differentiated and unfavourable treatment of consumers who use automated systems compared to consumers who do not. On the other hand, the prohibition that the entrepreneur prevents the use of virtual assistants for contracting. But in neither of its two variables is the principle absolute. In fact, the debate on whether a genuine 'right to use' ADM systems should be recommended and crystallized into duties on the trader not to prevent, limit or restrict has been complex and remains open. Competing interests are pitted against each other and do not facilitate a one-colour solution.

The effective exercise of an eventual right to use ADM systems for contracting by consumers would require, first, preventing the use of technological, operational or design measures that block, deter or disable the use of virtual assistants (*blockers*); and, second, implementing contractual, technological and design solutions that facilitate the virtual assistant to perform the necessary actions under equivalent conditions. Digital spaces (websites, applications and other digital user interfaces) should be designed in such a way that they do not pose a barrier to automated systems or, moreover, that they are *ADM-friendly, i*.e. suitable for use by digital assistants. For example, a digital assistant must be able to allow a digital assistant to 'use' a withdrawal button on a website (and the digital assistant must have this functionality). Another important element which is already expressly provided for in the regulation and which will be key for virtual assistants to play their role is that the information to be provided by traders must be available in machine-readable form and, of course and cumulatively, in a form which is intelligible to the consumer (Art. 14 RSD)[52]. This is the

[52] Article 14(1) DSA, General conditions:
'Intermediary service providers shall include in their general terms and conditions information about any restrictions they impose in relation to the use of their service

only way to avoid *de facto* discrimination against consumers assisted by automated contracting systems.

The implementation of these technological and operational, design and programming measures involves costs and requires changes in communication channels, interfaces and contracting procedures. They could therefore become a burden for small companies, putting them at a disadvantage vis-à-vis established market players and large platforms. This disruptive effect on the market has to be taken into account in the final shaping of the principle of non-discrimination and *non-barrier*. But in addition, and from another perspective that applies equally to small and large entities, the use of automated systems can saturate the system, simultaneously block available offers without completing the transaction, alter prices or erroneously generate messages of non-availability (*bots* for purchasing tickets or tickets, assistants that keep multiple transactions pending simultaneously, *bots* that saturate the system and block it, automated systems that multiply bookings). The above examples illustrate that there may be cases where legal restrictions (and valid contractual prohibitions) may exist or be imposed on the use of AI systems to protect specific interests, such that their use becomes unlawful, inappropriate or unreasonable.

D. Rethinking paradigms to address digital vulnerability: towards a notion of algorithmic or ADM-related vulnerability

The use of ADM in and for contracting alters the a/symmetries between the parties, re-allocates the risks throughout the contract life-cycle, and dynamically re-balances the power relationships in the transactional context. As a consequence, algorithmic contracting invites the revisit of legacy paradigms and principles underpinning the classical notion of vulnerability. Concurrently, the use of ADM in transactional contexts aggravates certain vulnerabilities, and creates new ones, whereas it proves to mitigate or eliminate other vulnerability factors.

in respect of information provided by recipients of the service. This information shall include details of any policies, procedures, measures and tools used to moderate content, including algorithmic decision-making and human review, as well as the procedural rules of their internal complaint handling system. It shall be in clear, plain, intelligible, user-friendly and unambiguous language, and shall be made publicly available in an easily accessible and machine-readable format'.

Therefore, the interplay between algorithmic contracting and digital vulnerability is complex, multifaceted, and challenging. It goes beyond the concept of digital vulnerability. In fact, considering the source of the potential vulnerabilities, exploring a concept of algorithmic (or ADM-related) vulnerability would be promising and advisable. This ‘algorithmic vulnerability’ stacks on the notion of digital vulnerability. It builds on it but it adds a new layer of challenges. Algorithmic vulnerability naturally resides in the context where digital vulnerability emerges.

The notion of algorithmic vulnerability would acknowledge the impact of the use of ADM in the framework of the digital architecture and in digital relations. However, its challenges are distinct and lead to different vulnerability scenarios.

The vulnerability assessment needs to solve first the main legal issues arising from the use of ADM/AI system for contractual purposes. As expounded in this Paper, at least two rules are absolutely critical in laying the foundations for a legal framework enabling algorithmic contracting: legal recognition rule and attribution rule. A strong case for international uniform rules has been made. And the adoption of the MLAC by UNCITRAL responds to it with an articulated solution.

Only then, it can be explored the algorithmic contracting territory through the lens of vulnerability concerns. And the image displayed is complex, paradoxical, and still blurry. The use of ADM systems for contractual purposes leads to new forms of inequality and vulnerability risks as well as offers promising possibilities to re-equilibrate balances and repair failures that would mitigate the perceived vulnerabilities. The interplay between digital vulnerability and algorithmic contracting is two-sided. And a narrower notion of ‘algorithmic (or ADM-related) vulnerability’ emerges and should be more closely studied.