The Contractual Governance of AI between the Public and Private Sectors: Transparency and Explainability as Contractual Obligations?*

Federico D'Orazio

Table of contents

1. Introduction: Is the Governance of AI Shaped by Contracts?

Existing studies on the regulation of AI mainly focus on the different legislative approaches adopted by legal systems to govern its development and use. From a comparative law perspective, the three contrasting models of the European Union, the U.S., and China are often investigated, with emphasis on how regional legislation can produce extraterritorial effects that shape global trends in commercial practice[1]. In the EU, legal analysis is centred in particular on the provisions of the AI Act[2] and its risk-based

* Peer-reviewed article

[1] For a broad perspective on the ways the different approaches to market regulation established in the EU, the U.S. and China are reflected in AI (and, more generally, digital) regulation with extraterritorial effects, see F. Bignami - G. Resta, *Digital Extraterritoriality: A Comparative Law Perspective*, in G. De Gregorio - O. Pollicino - P. Valcke (eds), *The Oxford Handbook of Digital Constitutionalism*, OUP online edn., 18 dec. 2024.

[2] 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

approach developed through a mix of safeguards typical of product safety legislation and fundamental rights protection[3].

Beyond standard-setting organisations contemplated by the Regulation[4], comparatively less attention has been devoted to the role of private actors in shaping the governance of AI systems, with limited consideration of the implications stemming from the contractual arrangements established between AI providers and deployers[5]. The analysis of the effects produced by contracts on the governance of AI requires understanding the ways they function as regulatory instruments operating in the shadow of AI and data protection legislation[6], or as its substitute, in legal systems where

and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[3] M. Almada - N. Petit, *The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights*, in *Common Market Law Review*, 1, 2025, 85 ff.

[4] See, e.g., J. Laux - S. Wachter - B. Mittelstadt, *Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act*, in *Computer Law & Security Review*, July 2024, 105957.

[5] Notable exceptions have so far had a focus limited to the public sector, centring on public procurement contracts concluded between developers of AI systems and the public administration, and the implications they might have for transparency and accountability of automated decision-making processes carried out by public actors: R. Brauneis - E.P. Goodman, *Algorithmic Transparency for the Smart City*, in *Yale Journal of Law & Technology*, 2018, 163 ff.; D.K. Mulligan - K.A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, in *Berkeley Technology Law Journal*, 34(3), 2019, 773 ff.; C. Coglianese - E. Lampmann, *Contracting for Algorithmic Accountability*, in *Administrative Law Review Accord*, 6(3), 2021, 175 ff.; L.M. Ben Dor - C. Coglianese, *Procurement as AI Governance*, in *IEEE Transactions on Technology and Society*, 2(4), 2021, 192 ff.; D.S. Rubenstein, *Acquiring Ethical AI*, in *Florida Law Review*, 73(4), 2021, 797 ff.; J. Boughey, *Transparency in Outsourced Automated Decision-Making Systems*, in *Public Law*, 2, 2023, 206 ff.; R. Matulionyte, *Government Automation, Transparency and Trade Secrets*, in *Melbourne University Law Review*, 47(3), 2024, 716 ff.; A. Sanchez-Graells, *Digital Technologies and Public Procurement: Gatekeeping and Experimentation in Digital Public Governance*, Oxford, 2024, 73 ff. Beyond the public sector, other works have recently started focusing on private ordering by generative AI providers through user contracts and privacy policies: L. Edwards - I. Szpotakowski - G. Cifrodelli - J. Sangaré - J. Stewart, *Private ordering, generative AI and the 'platformisation paradigm': What can we learn from comparative analysis of model terms and conditions?*, in *Cambridge Forum on AI: Law and Governance*, 1(e2), 2025, 1 ff. With specific regard to AI supply chains involving multiple parties and their impact on algorithmic accountability, see also J. Cobbe - M. Veale - J. Singh, *Understanding Accountability in Algorithmic Supply Chains*, ACM Conference on Fairness, Accountability, and Transparency, June 12-15, 2023, Chicago, in *dl.acm.org* (accessed 28.03.2026).

[6] The expression "bargaining in the shadow of the law" generally reflects the idea that contracts can operate within the silences of the law, functioning as regulatory instruments or mechanisms of private ordering that create norms beyond state legislation. This typically occurs either when default rules allow private parties to deviate from statutory provisions, or when contracts position themselves in areas that are not otherwise regulated. AI procurement contracts seem to fall within the latter category (the GDPR, for instance, does not regulate the relationships among actors along the AI supply chain), with the distinctive feature, however,

regulatory interventions lack. This paper intends to start filling the gap in the literature by investigating how contractual agreements between AI providers and deployers influence the level of transparency of algorithmic decision-making, the effectiveness of individual rights to obtain explanations of automated decisions, and the allocation of risks and liability between the parties. Specifically, it explores the extent to which these contracts, by limiting the flow of information necessary to interpret and explain AI outputs, may define critical aspects of the governance of AI.

To identify the boundaries of this "contractual governance of AI", the article focuses on two main sets of research questions: the first illustrates the issues generated by contractual practices in AI procurement, while the second delves into the analysis of possible solutions, with particular attention to the European framework. They can be summarised as follows: 1. What is the role of contracts in the definition of the critical features of the governance of AI? What are the implications for individuals affected by automated decisions? 2. What countermeasures have legal systems implemented across the public and private sectors? Are there specific insights to be drawn in the EU from the enactment of the AI Act?

Accordingly, the article begins by describing the effects of the contractual arrangements established by AI providers and deployers through the analysis of the European Court of Justice's judgment in *Schufa*[7] (section 2). While the decision concerned the interpretation of art. 22 of the GDPR[8] on automated decision-making, it is argued that the facts of the case indirectly shed light on how private actors can create (through contracts) situations where their liability is limited or excluded, and explanation rights of affected persons are emptied of their effectiveness. The decision of the

that they may undermine the effectiveness of safeguards established under AI and data protection legislation. The notion of «bargaining in the shadow of the law» can be traced back to R.H. Mnookin - L. Kornhauser, *Bargaining in the Shadow of the Law: The Case of Divorce*, in *Yale Law Journal*, 88(5), 1979, 950 ff.; R. Cooter - S. Marks - R. Mnookin, *Bargaining in the Shadow of the Law: A Testable Model of Strategic Behavior*, in *Journal of Legal Studies*, 11(2), 1982, 225 ff. For a historical analysis of how the regulatory role of private actors evolved over time, and further consideration of contracts in the shadow of the law, see S. Grundmann - M. Grochowski, *The Creation of Norms: An Evolutionary View of European Contract Law*, in S. Grundmann – M. Grochowski (eds.), *European Contract Law and the Creation of Norms*, Cambridge, 2021, 31 ff. See also M. Grochowski, *Shadow Contract Law in the Platform Economy*, in F. Casarosa – M. Grochowski (eds.), *Enforcing Private Regulation in the Platform Economy*, Tübingen, 2025, 97 ff. (conceptualising the role of digital platforms as creators of alternative systems of contract rules).

[7] CJEU, C-634/21, *SCHUFA Holding AG* (2023) (hereinafter *Schufa*).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Court will serve as a starting point to expand the investigation beyond GDPR provisions and identify an autonomous contract law problem. The regulatory ambition of contractual agreements in this sector is further evidenced in section 2 by examining standard terms in contracts for commercially available AI services offered by leading companies in the market[9].

The paper then turns to the ways legal systems, within and outside the EU, have been reacting across the public and private sectors to the role played by contracts in the governance of AI (section 3). The measures adopted encompass model contract clauses and guidelines for the public procurement of AI systems as well as hard law provisions that potentially limit the contractual freedom of private actors. The latter approach is investigated on the basis of the EU AI Act[10] and its provisions that impose on providers a duty to share relevant information with deployers. Building on the previous section and on the interactions between the AI Act and Member States' general contract law rules, section 4 considers the position of affected persons vis-à-vis the obligations of providers and deployers under AI procurement contracts. Section 5 offers a conclusion, summing up the main results of the research and underscoring the need for further investigation on the influence of contractual arrangements on key aspects of AI governance.

2. Identifying and Illustrating the Problem: The ECJ's Judgement in *Schufa* and Standard Terms in AI Procurement Contracts

In its 2023 judgment in *Schufa*, the European Court of Justice interpreted art. 22 of the GDPR on automated decision-making[11], extending its application to cases where automated decisions significantly affecting data subjects are the result of a process involving two parties: one carrying out

[9] This paper takes into account standard (business) terms found in contracts for commercially available AI services offered by Amazon, Meta, Microsoft, and OpenAI: see *supra* n 23 ff.

[10] A first assessment of the impact of the AI Act on contracts was carried out (when the Regulation was still in a drafting stage) by T. De Graaf - G. Veldt, *The AI Act and Its Impact on Product Safety, Contracts and Liability*, in *European Review of Private Law*, 30(5), 2022, 818 ff.

[11] Art. 22(1) of the GDPR establishes the right of data subjects not to be subject to decisions based solely on automated processing of their personal data which produce legal effects or similarly significantly affect them. The scope of application of this right is however limited by the broad exceptions enumerated in para. 2 of the provision. Moreover, the data controller has to implement suitable measures to safeguard the rights of data subjects and ensure the exercise of their rights to obtain human intervention, express their point of view, and contest the decision (para. 3).

the processing of personal data by automated means and the other adopting the final decision relying decisively on the results of such processing[12]. The relevance of the ruling is appreciated when considering the implications of the applicability of art. 22 in terms of safeguards available to data subjects. In particular, among the GDPR provisions that come into play, art. 15(1)(h) entitles data subjects to obtain an explanation of automated decisions by ensuring their access to meaningful information about the logic involved in the process (the so-called right to an explanation)[13]. The existence of such a right under art. 15 of the GDPR was recently acknowledged by the ECJ in *Dun & Bradstreet*[14] and a similar protection is now established in the

[12] The ECJ concluded that «Article 22(1) of the GDPR must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes "automated individual decision-making" within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person» (para. 74).

[13] Before recent clarification by the ECJ, an academic debate developed around the interpretation of art. 22 of the GDPR and the existence of a right to an explanation of automated decision-making, investigating the scope, function, and usefulness of the safeguards envisioned by the GDPR. For the essential terms of the debate, cf. B. Goodman - S. Flaxman, *European Union Regulations on Algorithmic Decision-Making and "a Right to Explanation"*, in *AI Magazine*, 38(3), 2017, 50 ff.; L. Edwards - M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for*, in *Duke Law & Technology Review*, 16(1), 2017-2018, 18 ff.; S. Wachter - B. Mittelstadt - L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7(2), 2017, 76 ff.; G. Malgieri - G. Comandé, *Why a Right to Legibility of Automated Decision Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7(4), 2017, 243 ff.; A.D. Selbst - J. Powles, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 7(4), 2017, 233 ff.; M. Kaminski, *The Right to Explanation, Explained*, in *Berkeley Technology Law Journal*, 34(1), 2019, 189 ff.; P.B. de Laat, *Algorithmic Decision-Making Employing Profiling: Will Trade Secrecy Protection Render the Right to Explanation Toothless?*, in *Ethics and Information Technology*, 24(17), 2022, 1 ff.

[14] CJEU, C-203/22, *CK v Dun & Bradstreet Austria GmbH* (2025) (hereinafter *Dun &Bradstreet*). The case concerned the information that an Austrian credit scoring company (Dun & Bradstreet) had to provide to a data subject under art. 15(1)(h) of the GDPR after a mobile telephone operator had denied her its services, based on the automated assessment of her credit solvency carried out by the first company. The ruling is worth mentioning because it confirmed the existence of a right to explanation under the GDPR and clarified its relationship with trade secrets, acknowledging the need to balance the two conflicting rights as to ensure data subjects' access to meaningful information without compromising their confidential nature. Defining the scope of application of art. 15, the Court also stated that «the "meaningful information about the logic involved" in automated decision-making [...] must describe the procedure and principles actually applied in such a way that the data subject can understand which of his or her personal data have been used in the automated decision-making at issue, with the complexity of the operations to be carried out in the context of automated decision-making not being capable of relieving the controller of the

AI Act, whose art. 86 introduces the right of affected persons to obtain explanations of the role of AI outputs in decision-making procedures[15].
For the purposes of this article, however, the ECJ's judgment in *Schufa* mainly serves as a benchmark that helps us identify and illustrate the role of contractual agreements in the governance of AI. This can be done by briefly summarising the facts of the case: Schufa, a German credit scoring company, calculated a score reflecting the creditworthiness of a data subject based on the automated processing of her personal data, and then communicated it to a third party (a bank) who relied on such score to decide whether to conclude a contract with the data subject. Being denied a loan on these grounds, the data subject was faced with unsatisfactory options: she could not obtain meaningful information about the logic involved in the automated decision either from the bank nor Schufa, thus being unable to contest it and being forced to suffer the negative consequences. In particular, the bank could not provide the relevant information as they were not in its possession, having outsourced the automated processing of personal data to Schufa; the latter, on the other hand, was not obliged to make such information available because it had not taken any decision towards the data subject (Schufa had only calculated a score and transmitted it to the bank)[16]. Acknowledging the risk of creating a vacuum in legal protection that would have defied GDPR safeguards against automated decision-making, including the right to explanation under art. 15, the ECJ expanded the scope of application of art. 22 as to include processes segmented between different actors,

duty to provide an explanation» (para. 61). For the purposes of this article, this ruling adds another element to be considered, that is the extent to which broad trade secrets protections established in procurement contracts can further restrict information flows towards deployers and affected persons. For further consideration of the limits posed by trade secrecy, see, with respect to public procurement contracts, C. Coglianese – E. Lampmann, *Contracting for Algorithmic Accountability*, cit., 184 ff.

[15] Specifically, art. 86(1) of the AI Act provides: «Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system [...], and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken». Para. 3 states that the provision applies only when the right to explanation is not otherwise provided for under EU law. For an analysis of art. 86 of the AI Act and its relationship with GDPR safeguards, see M. Brkan - H. Palčič Vilfan, *Art. 86 Right to Explanation of Individual Decision-Making*, in C.N. Pehlivan - N. Forgó - P. Valcke (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, 2025, 1209 ff; M. Kaminski – G. Malgieri, *The Right to Explanation in the AI Act*, in *papers.ssrn.com* (accessed 6 November 2025).

[16] The same reconstruction is offered by the ECJ in *Schufa*, cit., at para. 63.

enabling the data subject to exercise her rights against Schufa[17].
Going beyond the interpretative solution adopted by the Court under the GDPR, it seems necessary to consider the factors that in similar cases lead to the unavailability of legal remedies for persons affected by automated decisions. Analysing the case from a contract law perspective, it might be suggested that the unsatisfactory outcome stemmed from the arrangement of interests established in the contract stipulated by Schufa with the bank. The contract under which the first party agreed to calculate scores by automated means and communicate them to the bank evidently included no obligation to transfer the information necessary to provide explanations to data subjects; this allowed private actors to circumvent GDPR provisions, avoiding liability under the Regulation and emptying data protection safeguards of their effectiveness.
From this viewpoint, it emerges how contractual decisions over the flow of information necessary to interpret and explain AI outputs can define critical elements of the governance of AI. To ensure that AI systems are used in a transparent manner by deployers, that liability is fairly distributed between providers and deployers, and that affected persons can exercise their rights under the GDPR and the AI Act, it is essential to take into account this underexplored regulatory layer made of contracts and its relationship with existing legislation. After all, in *Schufa*, the parties (by excluding information transfers between them) were able to establish an arrangement that perfectly aligned with their commercial interests, limited their obligations under the GDPR, and hindered data subjects' safeguards and remedies. The interpretative solution adopted by the Court of Justice – to extend the application of art. 22 so that the data subject could exercise her rights against Schufa – represents a useful measure only when the provision applies. As such, it does not address a problem that goes beyond GDPR rules and can be seen as contractual in nature.
It seems possible to think of situations like those that gave rise to *Schufa* as cases concerning a procurement contract under which a party, the "supplier" (a «provider» under the EU AI Act)[18] procures to another

[17] The lack of effective safeguards under circumstances similar to those in *Schufa*, notwithstanding the existence of a decision solely based on automated processing of personal data significantly affecting data subjects, represents the underlying justification of the expansive interpretation of art. 22 of the GDPR proposed by the ECJ. See *Schufa*, cit., para. 61: «in circumstances such as those at issue in the main proceedings, in which three stakeholders are involved, there would be a risk of circumventing Article 22 of the GDPR and, consequently, a lacuna in legal protection if a restrictive interpretation of that provision was retained».

[18] According to art. 3, n. 3, of the AI Act, a provider is «a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market

subject, the "buyer", an AI system, output, or, more generally, an AI-based service, so that the latter (qualified as a «deployer» under the AI Act)[19] can use it to adopt significant decisions concerning third parties, the "affected persons". This structure appears broad enough to cover situations regulated by the GDPR[20] and the AI Act, and finds correspondence in the facts of other cases recently adjudicated by the ECJ[21]. Moreover, it offers a general framework to understand the agreements adopted in the contractual practice for commercially available AI or cloud computing services.

The standard terms found in these contracts[22] illustrate the regulatory ambition of private actors in the AI sector. These clauses typically limit, or entirely exclude, providers' liability, establish damages caps[23], deny liability

---

or puts the AI system into service under its own name or trademark, whether for payment or free of charge».

[19] Art. 3, n. 4, of the AI Act defines a deployer as «a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity».

[20] In cases that fall under the scope of application of the GDPR, both the "supplier" and the "buyer" are generally «data controllers» under art. 4, n. 7, of the GDPR. This was the case in *Schufa*: see the first question raised by the Administrative Court of Wiesbaden as reproduced in *Schufa*, cit., para. 27 (defining Schufa as a «controller» and the bank as a «third-party controller» to which the score is transmitted). It seems also possible to qualify the supplier as a «data processor» (cf. art. 4, n. 8, of the GDPR) operating on behalf of the data controller (the buyer adopting the final decision). In all cases, the «data subject» (as defined in art. 4, n. 1, of the GDPR) is an "affected person" under the proposed scheme.

[21] See *Dun & Bradstreet*, cit. The facts of the case are structured similarly to those in *Schufa*, cit.: a credit scoring company ("the supplier") provided a score to a mobile telephone company ("the buyer"), which then used that score to decide whether to enter into a contract with a consumer ("the affected person").

[22] A comprehensive analysis of the terms included in contracts for cloud computing services (and how they evolved over time) is carried out by the contributions in C. Millard (ed.), *Cloud Computing Law*, Oxford, 2021: J.D. Michels - C. Millard - F. Turton, *Standard Contracts for Cloud Services*, 49 ff.; W.K. Hon – C. Millard - I. Walden - C. Ward, *Negotiated Contracts for Cloud Services*, 100 ff.; N. Gleeson – I. Walden, *Placing the State in the Cloud: Issues of Data Governance and Public Procurement*, 421 ff.

[23] See, e.g., para. 14 of the OpenAI Services Agreement, May 31, 2025, in *openai.com* (accessed 6 November 2025); and para. 8 of Meta Platforms Technologies Products Commercial Terms, January 1, 2025, in *meta.com* (accessed 6 November 2025), establishing: «(i) MPT Products are provided "as is" for commercial use and we make no representations or warranties about commercial use of MPT Products; (ii) we make no representations or guarantees that MPT Products always will be safe, secure, or error-free, or that it will function without disruptions, delays or imperfections; (iii) we expressly disclaim any liability for any commercial use, whether of a MPT Product dedicated solely to commercial use or of a MPT Product used both for commercial and personal uses; and (iv) we also disclaim all warranties, whether express, implied, or statutory, oral or written, including the implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement». See also

for harms caused to third parties as a consequence of the use made of the services by the deployer, and exclude warranties in favour of the latter[24]. Also, they do not provide for transfers of information that would enable deployers to interpret and explain AI outputs, prohibit disclosures to third parties of information obtained under the agreement by the deployer[25], and establish broad trade secrets protection, for example by forbidding reverse engineering[26].

Considering that the contents of these agreements are usually not open to individual negotiation, there seems to be a similarity with the drafting techniques of online consumer contracts and the terms of service of online platforms[27]. When it comes to AI services, a worrying difference is, however, that the agreements are intended to be applied (not only to consumers but also) to businesses and public administrations[28], thus

para. 9 of the AWS Customer Agreement, September 9, 2025, in *aws.amazon.com* (accessed 6 November 2025); and, for Microsoft Azure products, para. 6 of the Microsoft Online Subscription Agreement, March 2019, in *azure.microsoft.com* (accessed 6 November 2025).

[24] See OpenAI Services Agreement, cit., para. 13.1. (excluding indemnification in favour of the customer for damages payable to a third party when the third-party claim depends on the applications made of the services by the customer and it would not have arisen but for such customer application); AWS Customer Agreement, cit., para. 7 (claiming that: «[t]o the extent permitted by applicable law, you [the buyer of the service] will defend, indemnify, and hold harmless us, our affiliates and licensors [...] from and against any Losses arising out of or relating to any third-party claim concerning [...] your or any End Users' use of the Services»); Supplemental Meta Platforms Technologies Terms of Service, April 29, 2025, in *meta.com* (accessed 6 November 2025), para. 5.5.e (establishing: «To the maximum extent permitted by applicable law, you agree to defend (at our request), indemnify and hold harmless Meta and its affiliates from and against all claims, liabilities, damages, losses, and expenses [...] arising out of or in any way connected with [...] your purchase or use of the MPT Products»); Microsoft Online Subscription Agreement, cit., para. 4.

[25] See, e.g., AWS Customer Agreement, cit., para. 11.9.; OpenAI Services Agreement, cit., para. 7.

[26] Reverse engineering is usually considered a lawful acquisition of trade secrets under existing legislation: see, e.g., art. 3(1)(b) of the EU Trade Secrets Directive (dir. 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure). Recital 16 contemplates, however, the possibility for the parties to a contract to dispose differently. For one example, see OpenAI Services Agreement, cit., para. 3.3.

[27] This similarity could probably be explained by observing that many of the leading companies in the AI sector originally were (or still are) online or social media platforms used to govern users' interactions through contracts (that is the case, for example, of Amazon or Meta). On the regulatory role of contracts within the platform economy, see M. Grochowski, *Shadow Contract Law in the Platform Economy*, cit., 97 ff.

[28] The standard contractual terms are envisioned by providers as applicable also to government bodies. See, e.g., AWS Customer Agreement, cit., para. 11.12, (stating that «the Services and AWS Content are provided to the U.S. Government as "commercial services," "commercial computer software," "commercial computer software documentation," and "technical data"

operating in a context where consumer law restrictions on contractual clauses are not applicable. In some limited circumstances, adaptations of the terms might be available for public actors, should they engage in individual negotiations and reach an agreement with the provider[29]. The market standing of these companies, however, might lead to the alternative of adapting to the available terms or renouncing the products they offer, settling for lower quality and performance.

To the extent that AI services are acquired by deployers under the conditions of procurement contracts unilaterally drafted by providers, there is a risk of seeing unchallenged their power to shape the governance of AI through contractual provisions, with relevant implications on the allocation of liability between providers and deployers, the effectiveness of explanation rights, and the level of transparency of automated decision-making across the public and private sectors.

3. Tracing the Reactions of Legal Systems Across the Public and Private Sectors: Model Contractual Clauses, Guidelines, and Legislative Provisions

Legal systems have been reacting to the way procurement contracts shape the governance of AI through different strategies. A first type of solution is specific to the public sector and envisions the procurement powers of the public administration as tools that can orient the governance of AI towards the values of transparency and accountability, thus challenging the monopoly of providers over the terms and conditions under which AI systems are made available. This approach finds support in academic research that considers AI public procurement as governance[30] and has

with the same rights and restrictions generally applicable to the Services and AWS Content. If you are using the Services and AWS Content on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, you will immediately discontinue your use of the Services and AWS Content»). See also Supplemental Meta Platforms Technologies Terms of Service, cit., para. 5.11. (stating: «We provide the MPT Products for public sector end use, including U.S. Government end use, with the same rights as all other end users pursuant to these Supplemental Terms. If a public sector entity, including a U.S. Government entity, has a need for any additional rights, it must negotiate directly with Meta to determine if the parties can negotiate an acceptable amendment to these Supplemental Terms that must be included in any applicable contract or agreement»).

[29] See previous footnotes.

[30] See R. Brauneis – E.P. Goodman, *Algorithmic Transparency for the Smart City*, cit., 163 ff.; D.K. Mulligan – K.A. Bamberger, *Procurement as Policy*, cit., 773 ff.; C. Coglianese – E. Lampmann, *Contracting for Algorithmic Accountability*, cit., 181 ff.; L.M. Ben Dor – C. Coglianese, *Procurement as AI Governance*, cit., 193 ff.; D.S. Rubenstein, *Acquiring Ethical AI*, cit., 797 ff.

so far relied on the development of model contract clauses envisioning contractual safeguards to be implemented when public administrations acquire AI systems.

Model contract clauses have been adopted at different administrative levels in Australia, the EU, and the U.S.: while in Australia the initiative was taken by the Digital Transformation Agency of the Australian Government[31], in the EU, similar clauses were drafted upon request of the European Commission, taking advantage of the experience previously developed by the City of Amsterdam[32] and now focusing on the public procurement of high-risk AI systems as defined in the EU AI Act[33]. In the U.S., standard terms for AI public procurement have been developed mostly by state and local administrations, including the Washington State Department of Enterprise Services[34], and a group of municipalities and state administrations led by the City of San Jose (California) under the name of «Government AI Coalition»[35]. So far, the U.S. Federal Government has not made specific contract clauses available to federal agencies but has provided guidelines within presidential memoranda with direct implications for procurement contracts[36]. Guidelines for the public procurement of AI systems had also been published by the Government of the United Kingdom in 2020, identifying the main questions that public administrations must address when drafting AI procurement contracts[37].

---

[31] Australian Government, Digital Transformation Agency, *Artificial Intelligence (AI) Model Clauses*, version 2.0, March 2025, in *buyict.gov.au* (automatic download, accessed 14 November 2025), hereinafter *Australian model clauses*.

[32] See Gemeente Amsterdam, *Modelbepalingen voor gemeenten voor verantwoord gebruik van Algoritmische toepassingen*, in *amsterdam.nl* (accessed 14 November 2025), hereinafter *Amsterdam model clauses*.

[33] See European Commission, Public Buyers Community, *Model contractual clauses for the public procurement of High-Risk AI*, February 2025, in *public-buyers-community.ec.europa.eu* (accessed 14 November 2025), hereinafter *EU model clauses*. Similar clauses have been developed also for non-high-risk AI (available at the same link). For a critical evaluation of the definition of high-risk AI systems under art. 6 of the AI Act, see, among others, A. Bertolini - F. Fedorczyk - M.M. Mollicone - G. Migliora, *The Brussels Sphinx's Riddle. What is a high-risk AI System?* in *Rivista di diritto dei media*, 3, 2025, 150 ff.

[34] Washington State, Department of Enterprise Services, *Generative AI Contract Clauses for IT Procurement Contracts for Washington State Agencies*, April 1, 2025, in *des.wa.gov* (accessed 14 November 2025).

[35] GovAI Coalition, *Addendum: Requirements for AI systems*, in *sanjoseca.gov* (accessed 14 November 2025), hereinafter *GovAI Vendor Agreement*.

[36] See Executive Office of the President, OMB, Memorandum M-25-21, April 3, 2025; and Memorandum M-25-22, April 3, 2025. For a broader perspective on the current U.S. approach to AI, see also Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, January 23, 2025.

[37] UK Government, *Guidelines for AI Procurement*, 8 June 2020, in *gov.uk* (accessed 14

Although reflecting the very different approaches of these legal systems towards AI regulation[38], the solutions proposed for the public procurement of AI largely converge on important aspects. It can be anticipated, for example, that the contents of model clauses and guidelines are strikingly in contrast with the terms unilaterally drafted by providers for commercially available AI services. Among these instruments, there seems to be a shared attention towards the availability of information that enables explanations of automated decisions as well as transparency and accountability of decision-making processes, the identification of providers' duties and ongoing obligations beyond the mere transfer of the product or procurement of the service, and the establishment of warranties in favour of buyers.

Starting with the provisions on information transfers between suppliers (AI providers) and buyers (public actors), model contractual clauses and guidelines generally require the former to communicate all information, technical and non-technical, which allows the latter to interpret and explain AI outputs[39]. In some cases, it is specified that suppliers need to ensure the buyer's understanding of «the logic behind an individual output from the AI System» and «which features of the AI System contributed to the output»[40]. These provisions might be applicable upon request of the buyer or with respect to each AI output[41], thus establishing an ongoing duty of the supplier to assist public actors in providing clear and meaningful explanations[42]. Significantly, upon transfer of such information, the

November 2025), hereinafter *UK Guidelines*.

38 This emerges, for example, in the different degree of detail found in the *EU model clauses*, cit. – that largely reflect the provisions of the EU AI Act – when compared to the vaguer and principle-based *UK Guidelines*, cit., and U.S. Memorandum M-25-22, cit. Interestingly, the *Australian model clauses*, cit., are as detailed as the European ones (offering in some cases even broader safeguards), notwithstanding the absence of an encompassing legislation specifically devoted to AI in the Australian legal system.

39 *EU model clauses*, cit., art. 14.1. This provision largely reproduces art. 5 of the model clauses developed by the City of Amsterdam: see *Amsterdam model clauses*, cit., art. 5. Similar terms are also found in *Australian model clauses*, cit., art. 5.3.2.; and *GovAI Vendor Agreement*, cit., art. 9. Explainability and transparency are factors that public administrations need to take into account when procuring AI systems also under the *UK Guidelines*, cit.: see, in particular, «considerations» nn. 7, 8, and 10. Under the U.S. Presidential Memorandum M-25-22, «agencies, are encouraged, where appropriate, to prioritize obtaining documentation that facilitates transparency and explainability, and that ensures an adequate means of tracking performance and effectiveness for procured AI»: Memorandum M-25-22, cit., 6.

40 *Australian model clauses*, cit., art. 5.3.2.

41 *Ibid.*

42 *EU model clauses*, cit., art. 14.1. See also *UK Guidelines*, cit., consideration n. 10, devoted to ensuring «extended communication and information sharing between the buyer and supplier», «knowledge transfer and training», and «ongoing support». *Australian model clauses*, cit., notes

supplier grants the buyer the right to disclose it to affected persons to the extent necessary to explain automated decisions[43]. With respect to the intellectual property rights covering the AI system or the training datasets, the supplier must grant (or procure to) the buyer either the acquisition of such rights, or a non-exclusive licence over them[44].

Furthermore, model clauses and guidelines hold suppliers responsible for the development and implementation of AI systems. Accordingly, they must ensure that the systems comply with existing legislation and are designed in a way that guarantees sufficient transparency[45], with tools allowing deployers to oversee and monitor their activities[46]. Suppliers must also warrant that the systems do not infringe third parties' intellectual property rights[47], are suitable for the intended use of the public administration, and are free from any material defect in design[48]. More generally, suppliers are called to establish and implement risk management systems[49] as well as indemnify public administrations for third parties' claims concerning the infringement of IP rights and the violation of data protection rights «or equivalent rights» that stem from the use of the procured AI system or

sub art. 5.3.2., contemplate the possibility for public administrations to request the indication of the «key factors that led to the AI system to arrive to a particular result» and «the changes to the input that must be made to arrive at a different output» as well as information concerning the training datasets, technical information about the AI system, and even the source code (art. 7.2.). On these further information requirements, cf. *EU model clauses*, cit., arts. 4, 5, 14, and 17; Washington State, *Generative AI Contract Clauses*, cit., 5 (concerning access to «training data; algorithm; inputs; outputs; and audit trails, logs, or hashes»).

43 *Australian model clauses*, cit., art. 5.3.3.; *EU model clauses*, cit., art. 14.2.

44 *Australian model clauses*, cit., art. 10; *EU model clauses*, cit., art. 16 (concerning IP rights over datasets). *UK Guidelines*, cit., 19; and Memorandum M-25-22, 5, lit. e).

45 *Australian model clauses*, cit., art. 5.3.1; *EU model clauses*, cit., art. 6.1. («[t]he Supplier ensures that the AI System has been and shall be designed and developed in such a way that the operation of the AI System is sufficiently transparent to enable the Public Organisation to interpret the system's output and use it appropriately»).

46 *Australian model clauses*, cit., art. 5.1.1.; *EU model clauses*, cit., art. 7.1. See also *GovAI Vendor Agreement*, cit., art. 8 (ensuring that the supplies provider the administration «the means for a human to evaluate and override outputs of the AI system. The human evaluator must be able to override the outputs of the AI system and take precedence over all outputs»).

47 *Australian model clauses*, cit., art. 10.4.

48 *Ibid.* art. 2.7. See also the section on «Risk Mitigation» in *GovAI Vendor Agreement*, cit., 1-2 (requiring suitability of the AI system with its intended use by the public administration and compliance with all applicable laws and regulations); and *UK Guidelines*, cit. (encouraging public administration to clearly allocate risks and liability under the contract, holding suppliers responsible for «technical, security and quality assurance»).

49 *Australian model clauses*, cit., arts. 13 ff.; *EU model clauses*, cit., art. 2; *GovAI Vendor Agreement*, cit., 1-2; Washington State, *Generative AI Contract Clauses*, cit., 7.

datasets[50].

Considering these solutions from a broader perspective, it is noteworthy that legal systems do not contest the role of procurement contracts as the place where critical decisions about the governance of AI can be taken: oriented towards the commercial interests of providers or the public values of transparency and accountability, these contracts are acknowledged as the instruments that define the terms of acquisition and use of AI systems, allocate risks and liabilities among the actors involved, and shape the level of protection granted to affected persons. Regardless of who controls the drafting of their provisions, they represent the constitutive elements of a "contractual governance of AI". Indeed, model clauses and guidelines for the public procurement of AI do not seek to diminish the influence of contracts in this sector; rather, they challenge the monopoly of private actors over the contents of such agreements by emphasising the need for public actors to leverage their public procurement powers as to adjust contractual obligations to broader interests and values than those advanced by providers. Ultimately, these solutions rely on the regulatory potential of procurement contracts in an attempt to orient commercial practices towards public goals[51].

Model clauses, guidelines, and public procurement procedures, however, are instruments with a limited scope of application – concerning only the public sector –, and some doubts can be raised on their (at least current) capacity to shape commercial practices in markets where the supply is governed by a small number of companies applying their terms and conditions globally[52]. Nonetheless, the values and interests that these

[50] *EU model clauses*, cit., art. 18.1. explicitly mentions suppliers' liability for violation of data protection rights or «equivalent rights» (likely referring to rights under the AI Act, such as the right to an explanation under art. 86 as «equivalent» to the right under art. 15(1)(h) of the GDPR). See also *GovAI Vendor Agreement*, cit., 1 (stating that the «Contractor agrees to indemnify, defend, and hold harmless the [Agency] regarding any third-party action rising out of or related to (1) any breach of any representation or warranty of Company contained in this Addendum; (2) any breach or violation of any covenant or other obligation or duty of Contractor under this Addendum or under applicable law; (3) any third party Claims which arise out of, relate to or result from any act or omission of the Contractor related to the provision of an AI system; and (4) any violations or alleged violations of intellectual property rights»).

[51] See, e.g., C. Coglianese – E. Lampmann, *Contracting for Algorithmic Accountability*, cit., 181 ff.; D.S. Rubenstein, *Acquiring Ethical AI*, cit., 797 ff.

[52] For a critical evaluation of the limits of public procurement procedures as instruments of digital governance, see A. Sanchez-Graells, *Digital Technologies and Public Procurement*, cit., 73 ff. The Author observes, in particular, that «[t]he question is whether procurement could effectively operationalize digital regulation goals without simply transferring regulatory decisions to economic operators, either directly through tender design or the awarded public contract, or indirectly through the incorporation by reference or reliance on commercially

instruments convey are worth pursuing, even beyond the public sector. Although particular attention should be paid to AI applications in that context – to the very least, because of the higher number of persons potentially affected and the superior degree of trust inspired by public institutions –, the need for transparency, fair allocation of risks and liabilities, and respect for the rights of affected persons is felt also in the private sector, whenever significant decisions concerning third parties rely on AI outputs. Therefore, it could be argued that the contractual clauses envisioned for AI public procurement should represent a point of reference also for transactions between private companies. However, having highlighted the current distance of platforms' user agreements from such a standard[53], it is necessary to turn to legislative solutions that seem to promote a direct intervention on the consequences stemming from the conclusion of AI procurement contracts.

This different attempt at steering contracts towards public values, based on hard law provisions, is arguably found in the EU AI Act. Albeit without clearly envisioning the implications for procurement contracts, this Regulation takes into consideration the flow of information between providers and deployers of high-risk AI systems in a way that inevitably affects the contents of contractual agreements. Art. 13, in particular, establishes the duty of providers to communicate to deployers information necessary to interpret and explain AI outputs. Such information is to be conveyed in the instructions for use of the supplied AI system, covering at least «the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output» and «information to enable deployers to interpret the output of the high-risk AI system and use it appropriately»[54]. In light of the reference to the

determined standards and practices» (76-77).

[53] See section 2.

[54] See respectively art. 13(3)(b)(iv) and (vii) of the AI Act. Confirming the duty of providers to transfer relevant information to deployers, see also art. 26(9)of the AI Act (concerning the obligations of deployers and stating that «[w]here applicable, deployers of high-risk AI systems shall use the information provided under Article 13 of this Regulation to comply with their obligation to carry out a data protection impact assessment». For a critical analysis of art. 13 of the AI Act, see M. Busuioc - D. Curtin - M. Almada, *Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act*, in *European Law Open*, 2(1), 2023, 91 ff. (adopting a critical stance on the ability of this provision to ensure adequate transparency for users). Within the AI Act, significant information duties are imposed also on the providers of general-purpose AI systems under art. 53(1)(b). Such information, listed in Annex XII, must be made available to «providers of AI systems who intend to integrate the general-purpose AI model into their AI systems» as to «enable providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model and to comply with their obligations pursuant to this Regulation».

explanation of AI outputs, the information duties under art. 13 should be read together with art. 86 – establishing the right to explanation under the AI Act –, whose judicial interpretation will indirectly define the minimum of information subject to disclosure from providers to deployers[55].

From a contract law perspective, the provisions of the AI Act that impose upon providers specific duties towards deployers – such as the duty to disclose information concerning the functioning of the AI system – seem to have an impact on contracts stipulated between the same parties. Focusing on information duties, art. 13 of the AI Act can be interpreted as a regulatory source of contracts for the procurement of high-risk AI systems, affecting their contents so that their conclusion entails by law – as ancillary to the main obligation to procure the AI system or output – the contractual obligation of the supplier to transfer to the buyer the information necessary to interpret and explain AI outputs; failure to perform such obligation would position the provider in breach of contract, with all the implications contemplated by Member States' general contract law rules.

Through these lenses, the attempt of the AI Act to shape the governance of AI emerges as depending, among other things, on contract regulation and its effects on private parties' freedom to determine the terms of procurement agreements. The AI Act approach – reproduced in legislative initiatives of some U.S. States[56] – differs from the solutions based on model contractual clauses and guidelines for the public procurement of AI not only because of its wider scope of application (encompassing the private sector), but also because it exploits the strength of the law to establish specific obligations of providers under AI procurement contracts. Moreover, by regulating information flows between providers (suppliers) and deployers (buyers), the AI Act goes beyond the subject matter of GDPR provisions, which do not focus on information transfers between the different companies involved in the automated decision-making process[57]. Ensuring such communication of information should enable

[55] Art. 86 is likely to be interpreted in line with the reading provided by the ECJ of art. 15(1)(h) of the GDPR in *Dun & Bradstreet*, cit. (see *supra* n. 14).

[56] See, for example, the State of Colorado Bill SB 24-205 signed into law under the title of Consumer Protections for Artificial Intelligence. Sec. 6-1-1702 identifies information subject to disclosure from the provider to the deployer, including information necessary «to assist the deployer in understanding the outputs and monitor the performance of the high-risk artificial intelligence system» (6-1-1702(2)(c)).

[57] The absence of similar obligations under the GDPR, as already observed, led to the unavailability of rights and remedies in *Schufa*, cit. Lacking any suitable legal basis under the GDPR, the European Court of Justice could not intervene in that case by imposing such a duty upon Schufa (the supplier of the AI output) towards the bank; the Court could only enable the data subject to exercise her rights against that same company through an expansive

affected persons to exercise their rights directly against those adopting significant decisions on the basis of AI outputs (rather than against the suppliers of such outputs).

4. Contracts for the Procurement of High-Risk AI Systems and Third Parties in a European Private Law Perspective

The AI Act regulation of the relationship between providers and deployers – integrated with Member States' private law rules generally applicable to procurement contracts – seem to define the legal consequences of agreements on the procurement of high-risk AI systems. To this extent, the AI Act can be seen as a source of expansion of European contract law, now encompassing contractual figures concerning the transfer of rights over AI systems whose regulation partially relies on EU law.
Albeit the focus of this paper has been on contractual obligations to make available information enabling explanations of AI outputs (because of the relevance they have for the rights of affected persons), it is possible to imagine that many other requirements imposed on providers by the AI Act will start finding some correspondence in contractual agreements concerning high-risk AI systems. This does not necessarily mean, however, that the provisions of the AI Act can always be read as the source of contract regulation, establishing mandatory contractual obligations in the way it is proposed for information transfers. What seems to justify the distinction is whether the law (the AI Act) explicitly contemplates providers' duties as specifically owed to deployers: while this seems to be the case for the duty to transfer information necessary to interpret and explain AI outputs, the same might not be true in other instances[58]. Nevertheless, even when a mandatory obligation does not exist, contracting parties (especially deployers) might still be interested in finding ways to transpose the provisions of the AI Act within their contracts, presumably

interpretation of art. 22 of the GDPR.

[58] Notably, the AI Act grants private parties some flexibility to allocate responsibilities along the AI value chain. Under art. 25(1)(a) of the Regulation, «[a]ny distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances: (a) they put their name or trademark on a high-risk AI system already placed on the market or put into service, *without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated*» (emphasis added). According to para. 4 of the provision, the AI Office may develop «voluntary» model clauses for contractual agreements between providers and third parties that supply components or processed integrated in high-risk AI systems.

under the form of warranties[59].

Within this broader framework that encompasses the implications of the introduction of the AI Act for the development of European private law, it is here possible to focus only on a specific aspect, that is the position of the affected person vis-à-vis the contract for the procurement of high-risk AI systems. This allows us to provide a first assessment of their relationship under private law rules. It has been observed, indeed, that whenever the provider fails to disclose to the deployer information necessary to explain AI outputs, rights of affected persons to access such information become ineffective[60]. This usually prevents the individual from contesting the decision, leading to a stabilisation of its negative consequences. It follows that the relationship between the contractual agreement and the affected persons should be further investigated as to evaluate what remedies are available to latter.

With respect to the contract between the provider and the deployer, the affected person can be considered as a third party whose position is impacted on by the breach of contractual obligations, and, in particular, the supplier's obligation to disclose relevant information to the buyer. Considering the absence of a direct attribution of rights to the affected person under the agreement, it should first be excluded that the contract for the procurement of high-risk AI systems can represent a contract in favour of a third party[61]. Against this possibility, it appears decisive that,

[59] The adoption of a similar approach can be identified in the model contract clauses developed by the European Commission for the public procurement of high-risk AI systems (analysed in the previous section).

[60] After the ECJ's decision in *Schufa*, cit., this should not be the case when art. 22 of the GDPR applies, as the data subject could ask the relevant information to the party which has carried out the automated processing of personal data and then transmitted the results to a different actor adopting the final decision. The limited application of this provision (considering the broad exceptions it provides) may suggest however the need to consider the issue (also) from the perspective of private law rules.

[61] When introducing the topic of contracts in favour of a third party, a common starting point in legal scholarship is the principle of relativity of contracts as consolidated in contract law rules of European legal systems. For comparative law studies on the effects of contracts towards third parties, encompassing the experiences of England, France, Germany, and Italy, see, within an extensive literature, V.V. Palmer, *The Paths to Privity: The History of Third Party Beneficiary Contracts at English Law*, San Francisco, 1992; S. Whittaker, *Privity of Contract and the Tort of Negligence: Future Directions*, in *Oxford Journal of Legal Studies*, 16(2), 1996, 191 ff.; D. Nolan, *Reforming Privity of Contract Doctrine*, in M. Andenas - N. Jareborg (eds.), *Anglo-Swedish Studies in Law*, Uppsala, 1999, 288 ff.; B. Markesinis, *An Expanding Tort Law – The Price of A Rigid Contract Law*, in *Law Quarterly Review*, 103(3), 1987, 354 ff.; H. Kötz, *European Contract Law*, trans. G. Mertens - T. Weir, Oxford, 2017, 319 ff.; S. Whittaker, *Privity of Contract and the Law of Tort: The French Experience*, in *Oxford Journal of Legal Studies*, 15(3), 1995, 327 ff.; G. Alpa - A. Fusaro (eds.), *Effetti del contratto nei confronti dei terzi*, Milan, 2000; S. Vogenauer, *Gli effetti dei contratti verso i terzi: L'Avant-projet in una prospettiva comparatistica*, in M.T. Andenas - S.

in commercial practice, the parties of AI procurement contracts never express such intention, nor do they usually acknowledge the position of the several individuals against which the buyer, acting as a deployer, might adopt automated decisions in the future. Accordingly, the characterisation of affected persons as third parties directly entitled to request performance of contractual obligations proves to be unpersuasive.

A different approach could be developed qualifying the AI procurement agreement as a contract with protective effects towards third parties. The doctrine of *Vertrag mit Schutzwirkung für Dritte* was originally developed by German courts and scholars to overcome the characteristic rigidities of German tort law[62], ranging from the closed list (under § 823, I, BGB) of rights and interests whose injury give rise to the duty to provide compensation[63],

Diaz Alabart – B. Markesinis - H.W. Micklitz - N. Pasquino (eds.), *Liber amicorum Guido Alpa: Private Law Beyond the National Systems*, London, 2007, 1000 ff.; J. Neuner, *Der Schutz und die Haftung Dritter nach vertraglichen Grundsätzen*, in *Juristen Zeitung*, 3, 1999, 126 ff.; S. Grundmann - M. Renner, *Vertag und Dritter – zwischen Privatrecht und Regulierung*, in *Juristen Zeitung*, 8, 2013, 379 ff.; A. Di Majo, *La protezione del terzo tra contratto e torto*, in *Europa e diritto privato*, 2000, 1 ff.; E. Moscati, *I rimedi contrattuali a favore dei terzi*, in *Rivista di diritto civile*, 4, 2003, 357 ff.; L. Vagni, *Il contratto a favore di terzi nella comparazione «common law-civil law» dallo «ius commune» al diritto privato europeo*, in *Rivista trimestrale di diritto e procedura civile*, 4, 2005, 1195 ff.; G. Grisi, *Principio di relatività degli effetti contrattuali*, in *Enc. dir.*, *I tematici*, *Contratto*, Milan, 2021, 907 ff.; F. Toriello, *Gli effetti del contratto nei confronti dei terzi nell'esperienza inglese*, in *Contratto e impresa Europa*, 1, 2000, 80 ff.; A. Fusaro, *Gli effetti del contratto nella riforma del Code civil francese*, in *Rivista di diritto privato*, 2, 2017, 7 ff.; M. Feola, *Contratto e protezione del terzo*, in *Annuario di diritto comparato e di studi legislativi*, Naples, 2017, 803 ff.

[62] The emergence of the doctrine of contracts with protective effects for third parties is commonly linked to the rigidities of German tort law: see, e.g., K. Larenz, *Lehrbuch des Schuldrechts*, *I*, *Allgemeiner Teil*, 12th edn., München, 1979, 185 ff. (connecting the doctrine to the limits imposed on vicarious liability under § 831 BGB); D. Medicus, *Schuldrecht I*, *Allgemeiner Teil*, 14th edn., München, 2003, 377 ff. (arguing – similar to Larenz – that the first court decisions on contracts with protective effects for third parties were meant to overcome the BGB rules on vicarious liability); B. Markesinis - J. Bell - A. Janssen (eds.), *Markesinis's German Law of Torts*, 5th edn., Oxford and Portland, 2019, 97 (defining the *Vertrag mit Schutzwirkung für Dritte* as a contractual solution «devised to overcome the shortcomings of the German law of tort»); H. Kötz, *The Doctrine of Privity of Contract in the Context of Contracts Protecting the Interests of Third Parties*, in *Tel Aviv University Studies in Law*, 1990, 196. The connection of the doctrine to the peculiarities of German tort law has often represented an obstacle to its circulation in legal systems lacking those specific characteristics. For discussion of the German doctrine and critical evaluation of its possible reception in Italy, see C. Castronovo, *Obblighi di protezione e tutela del terzo*, in *Jus*, 1-2, 1976, 123 ff.; A. Di Majo, *La protezione del terzo tra contratto e torto*, cit., 14 ff.; G. Varanese, *Il contratto con effetti protettivi per i terzi*, Naples, 2004; M. Maggiolo, *Effetti contrattuali a protezione del terzo*, in *Rivista di diritto civile*, 1, 2001, 39 ff.; A. Somma, *L'esperienza tedesca*, in G. Alpa – A. Fusaro (eds.), *Effetti del contratto nei confronti dei terzi*, cit., 116 ff.; and, within the same book, G. Alpa – A. Fusaro, *L'esperienza italiana*, 18 ff.

[63] § 823, I, of the BGB can be invoked only when there is a violation of rights and interests concerning life, body, health, freedom, property or "some other right", § 823, II, extends liability to those cases where there is a breach of a legislative norm designed to protect a

and the resulting limitations on the recovery of pure economic loss[64], to the restricted scope of application of the rules on vicarious liability (under § 831 BGB)[65]. In this context, the doctrine has served the purpose of ensuring protection to third parties who found no remedy under tort law by expanding the remit of contractual liability. Specifically, it operates through the extension of the applicability of *Schutzpflichten* ("duties to protect") beyond the parties of a contract – within which such duties are owed on the basis of the principle of good faith[66] – as to include third parties in a particular relationship with one of the contracting parties or in "proximity" to the performance of the contract[67]. As a result, third parties are not entitled to obtain performance of contractual obligations (as they would be if there was a contract established in their favour) but can claim compensation for the harms suffered as a consequence of a breach of the agreement under the more favourable rules governing contractual (rather than tortious) liability.

To delimit the scope of application of the doctrine, different requirements have been developed over time by courts, including (a) the proximity of the third party to the contractual obligation of the debtor, (b) the existence of a relationship between the creditor and the third party under which the former has a duty to protect the latter, and (c) the debtor's foreseeability of these elements at the time of the conclusion of the contract[68]. Transposing

specific interest. For an analysis of the characteristic features of German tort law, see B. Markesinis - J. Bell - A. Janssen (eds.), *Markesinis's German Law of Torts*, cit., 29 ff., and 72 ff.

64 Ivi, 97 ff. For an analysis on pure economic loss (encompassing especially England and Germany), see H. Kötz, *Economic Loss in Tort and Contract*, in *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 58(3), 1994, 423 ff.; B. Markesinis, *An Expanding Tort Law*, cit., 354 ff.

65 See B. Markesinis - J. Bell - A. Janssen (eds.), *Markesinis's German Law of Torts*, cit., 117 ff.

66 The German theory of *Schutzpflichten* can be traced back to H. Stoll, *Abschied von der Lehre von der positiven Vertragsverletzung*, in *Archiv für die civilistische Praxis*, 136(3), 1932, 257 ff. (introducing the distinction between *Leistungsinteresse* and *Schutzinteresse*). For an analysis of the origins of this theory and its attempt to overcome the doctrine of *positiven Vertragsverletzung* that had been previously elaborated by Hermann Staub, see, among many others, C. Castronovo, *Obblighi di protezione e tutela del terzo*, cit., 128 ff.; M. Feola, *Contratto e protezione del terzo*, cit., 806 ff.; G. Varanese, *Il contratto con effetti protettivi per i terzi*, cit., 14, *supra* n. 8.

67 The doctrinal conceptualisation of the *Vertrag mit Schutzwirkung für Dritte*, that, among other things, allowed to clearly distinguish this figure from the one of contracts in favour of third parties (originally relied upon by German courts in the first attempts to grant contractual remedies), is owed, in particular, to Karl Larenz, Joachim Gernhuber and Claus-Wilhelm Canaris. For a critical evaluation of the different positions adopted by these Authors with respect to the legal basis justifying contracts with protective effects for third parties under the BGB, see C. Castronovo, *Obblighi di protezione e tutela del terzo*, cit., 132 ff.

68 See K. Larenz, *Lehrbuch des Schuldrechts*, cit., 187 ff.; B. Markesinis, *An Expanding Tort Law*, cit., 362 ff.; D. Medicus, *Schuldrecht*, cit., 377 ff.; D. Martiny, *Plichtenorientierter Drittschutz beim Vertrag mit Schutzwirkung für Dritte – Eingrenzung uferloser Haftung*, in *Juristen Zeitung*, 1, 1996, 21

these requirements to the cases that arise from the supplier's breach of AI procurement contracts, it would be possible to see them satisfied: (a) the affected person is in proximity of the contract, having an interest in the performance of the agreement, as the supplier's failure to perform the information transfer to the deployer will hinder his/her right to obtain an explanation of the automated decision and contest it; (b) the affected person and the buyer are in a relationship under which the latter must protect the former (the latter being either a deployer or a data controller adopting an automated decision concerning the affected person); (c) the supplier (either a provider or a data controller) is in the position to foresee that the AI system or output procured to the buyer will be used to adopt significant decisions towards third parties.

The fulfilment of the last requirement, in particular, could be demonstrated whenever procurement contracts contemplate the intended uses of the supplied AI systems or outputs, thus allowing the supplier to indirectly identify the category of individuals potentially affected by the AI applications. Regardless of an explicit mention of possible AI applications within the agreement, the requirement could be deemed satisfied in cases when the AI output supplied by the provider is clearly intended to shape the results of a decision-making process carried out by the buyer. The existence of such circumstances may also be inferred from the identity of the contracting parties and the type of commercial activities they carry out. Considering, for example, the facts in *Schufa*, whether it was stated in the contractual agreement or not, it seems reasonable to believe that a credit scoring company assessing the creditworthiness of individuals can expect its scores being used for decisions concerning the stipulation of loan agreements when its contractual counterpart is a bank.

Furthermore, insofar as art. 13 of the AI Act expressly links the communication of relevant information to the need to explain AI outputs, it could be argued that it is the same legislative provision to implicitly acknowledge the relationship between the contractual obligation and the protection of affected persons (as they are the recipient of explanations under art. 86 of the AI Act). Adopting an interpretation of agreements for the procurement of high-risk AI systems as contracts with protective effects for third parties, the affected person would be entitled to claim compensation for damages suffered as a consequence of the breach of contract[69] directly against the supplier.

ff. (classifying in a structured manner the cases of application of the doctrine on the basis of the interests of the different parties involved, the types of duties arising from the contract, and their relationship with specific sets of cases adjudicated by German courts). See also G. Varanese, *Il contratto con effetti protettivi per i terzi*, cit., 38 ff.

[69] An important aspect, which cannot be fully addressed in this paper, is whether there is any

Some doubts could be raised, however, with respect to the necessity and usefulness of a similar doctrine to be consolidated in the European framework. The peculiar characteristics of the German law of torts that led to the expansion of contract-based claims and the judge-made doctrine of *Verträge mit Schutzwirkung für Dritte* might be read, in fact, as obstacles to its adoption as a model for the development of European private law[70]. Admittedly, other legal systems are used to envision the compensation of harm caused to third parties in proximity to a contract through tortious (rather than contractual) liability. It is the case, for example, of English law, whose traditional approach is exemplified by the well-known decision of the House of Lords in *Donoghue v. Stevenson*[71]. In that case – at the dawn of the rules concerning civil liability for defective products –, the consumer of a ginger beer containing a decomposed snail was found to have a claim under the rules of the tort of negligence directly against the manufacturer. This was possible – the Court argued – because the latter owed a duty of care to those who were in proximity (or in the neighbouring area) of the contract that party had concluded with the reseller. The comparative analysis of similar cases in England and Germany led renowned scholars to argue that English law had historically developed in a direction opposite to the one taken by German law: with the common law doctrines of privity of contract and consideration limiting the possibility of recognising

recoverable loss arising from the mere violation of the right to an explanation of automated decisions. In principle, it cannot be excluded outright, as the violation of such right usually implicates the consolidation of the negative consequences of the automated decision (first of all by hindering the possibilities to contest it). Nonetheless, demonstrating a direct causal nexus between the two might prove challenging. The issue is likely to be first assessed in cases where the provisions of the GDPR applies, allowing qualification of the violation of the right to an explanation under art. 15(1)(h) as an infringement of the Regulation, potentially triggering liability under art. 82. No clear indication on the recoverability of damages stemming from the mere violation of art. 15 has yet been given by the European Court of Justice.

70 For a similar conclusion, see A. Di Majo, *La protezione del terzo tra contratto e torto*, cit., 26.

71 [1932] SC (HL) 31. The link between the application of the tort of negligence in *Donoghue v Stevenson* and the German theory of *Vertrag mit Schutzwirkung für Dritte* is found, among many others, in H. Kötz, *The Doctrine of Privity of Contract in the Context of Contracts Protecting the Interests of Third Parties*, cit., 202; see also F. Toriello, *L'esperienza inglese*, in G. Alpa – A. Fusaro (eds.), *Effetti del contratto nei confronti dei terzi*, cit., 180 ff. For a detailed analysis of the case and critical evaluation of the ways the tort of negligence evolved after the decision of the House of Lords, see R.F.V. Heuston, *Donoghue v. Stevenson in Retrospect*, in *Modern Law Review*, 20(1), 1957, 1 ff.; J.C. Smith - P. Burns, *Donoghue v. Stevenson: The Not so Golden Anniversary*, in *Modern Law Review*, 46(2), 1983, 147 ff.; A.M. Linden, *The Good Neighbour on Trial: A Fountain of Sparkling Wisdom*, in *University of British Columbia Law Review*, 17(1), 1983, 67 ff.; A. Rodger, *Lord MacMillan's Speech in Donoghue v. Stevenson*, in *Law Quarterly Review*, 108(2), 1992, 236 ff.; F. Ferrari, *Donoghue v Stevenson's 60th Anniversary*, in *Annual Survey of International & Comparative Law*, 1(1), 1994, 81 ff.

contractual effects towards third parties[72], the solution had been to expand the tort of negligence in a manner that is almost specular to the way German law has extended the boundaries of contractual liability to circumvent the rigidities of the law of torts[73].
From a European private law perspective, therefore, it might be useful to think of intermediate solutions, for example distinguishing the relationship between the affected person and the buyer from the one the latter has with the supplier. On the one hand, the remedies available to affected persons against the buyer could be grounded on the specific type of relations entertained (contractual or extra-contractual)[74]; on the other hand, the buyer could hold the deployer liable for any damage stemming from breach of contract. This would allow affected persons to bring their claims against the closest subject (the buyer adopting an automated decision concerning them), making the same party accountable (and liable whenever there are recoverable losses) for having deployed AI systems without possessing the information necessary to explain their functioning. On the other hand, the buyer, having collected the different claims of affected persons due to its proximity to them, could then rely on contractual remedies against the supplier and recover any loss determined by the breach of contractual obligations to make relevant information available.

5. Conclusion

Existing studies on the regulation of AI systems have centred on the analysis of the different strategies adopted by legal systems, measuring the degree of their development on the basis of the existence and quality of legislative interventions. Departing from these premises, this paper has tried to shed light on the relevance of instruments other

[72] In English law, rights of third parties to a contract have been admitted since 1999 by virtue of the Contract (Rights of Third Parties) Act, adopted on the basis of the analysis carried out by Law Commission, *Privity of Contract: Contracts for the Benefit of Third Parties*, LAW COM No 242, June 1996. A similar path was followed by the Scottish legal system in 2017: cf. Contract (Third Party Rights) (Scotland) Act 2017, and Scottish Law Commission, *Review of Contract Law. Report on Third Party Rights*, SCOT LAW COM No 245, July 2016.

[73] See the comparative studies (with particular emphasis on pure economic loss) of H. Kötz, *The Doctrine of Privity of Contract in the Context of Contracts Protecting the Interests of Third Parties*, cit., 195 ff.; B. Markesinis, *An Expanding Tort Law*, cit., 355 ff.; S. Whittaker, *Privity of Contract and the Tort of Negligence*, cit., 191 ff. (focusing, in particular, on a comparison between English and French law)

[74] When the GDPR applies, the relevant legal basis would be art. 82 of the Regulation, with the violation of the right to an explanation under art. 15(1)(h) configuring an infringement of the GDPR potentially giving rise to liability (see *supra* n 69).

than the legislative ones as regulatory sources of the essential features of the governance of AI. In particular, contractual agreements between suppliers and buyers of AI systems and AI-based services appear as a regulatory layer influencing the allocation of risks and liability among the parties, the transparency of automated decision-making processes, and the effectiveness of explanation rights of affected persons. To the extent they are able to establish an arrangement of interests that circumvent legal rules and safeguards, they can be described as contracts operating in the shadow of data protection and AI legislation.

The role of procurement contracts in the governance of AI emerges from the analysis of recent cases that led the European Court of Justice to expand the scope of application of existing legal rules as a means to overcome the negative implications stemming from contractual agreements for third parties' rights[75]. The regulatory ambition of these instruments – and of the companies that deploy them – is made evident by the drafting techniques and standard terms adopted in contracts for commercially available AI and cloud computing services. Reacting to the monopoly of leading companies in the market over the contents of such agreements, otherwise offered to consumers, businesses, and even public administrations, appears therefore essential to safeguard transparency of automated decision-making processes and the rights of affected persons.

Admittedly, across different legal systems, it is already possible to identify several initiatives that seem to tackle some of the issues generated by contractual practices in AI procurement. Among these, the paper has considered model contractual clauses and guidelines for the public procurement of AI systems – adopted at different administrative levels in Australia, the EU, the United Kingdom, and the U.S. – as well as legislative interventions, such as the EU AI Act. With respect to both types of solutions, it is notable the absence of a direct opposition to the idea that contracts can represent the place where critical decisions over the features of the governance of AI are taken. Albeit relying on instruments with different strength and scope of application – public procurement powers on the one hand, and hard law provisions on the other –, both approaches are meant to challenge the exclusive control of AI providers over the terms of procurement contracts.

In the case of the EU AI Act, the provisions concerning the duty of providers to transfer to deployers information necessary to interpret and explain AI outputs seem to operate as a source of contract regulation, establishing a mandatory contractual obligation that cannot be waived by the parties, and whose violation determines a breach of contract. Insofar as this interpretation is embraced, the AI Act could be read as defining the (mandatory) legal regime of contracts concerning the procurement of high-risk AI systems. To this extent, the Regulation would be also advancing the boundaries of European contract law, establishing contractual figures

[75] See the analysis of the ECJ's decision in *Schufa*, cit., in section 2.

whose regulation can be traced back to EU law provisions.
Within this context of possible European private law expansion, further investigation should be carried out to conceptualise the role played by EU legislation in defining the relationship between affected persons and AI procurement contracts. Engaging with fundamental questions of contract law, such as those concerning the effects of contracts towards third parties, this paper has explored some possible solutions, drawing on the doctrines of contracts in favour of third parties and contracts with protective effects towards third parties. Ultimately, in order to enable affected persons to obtain remedies against the subject in their immediate proximity, it is suggested that they should be able to bring their claims against the deployer, holding the same party accountable for having adopted AI systems without adequate knowledge of their functioning and possession of information relevant to explain their outputs. At the same time, the deployer, being in a contractual relationship with a supplier who has breached its obligation to transfer such information, would be entitled to bring a claim against the latter and recover any loss suffered.
Recognising procurement contracts as the building blocks of a "contractual governance of AI" opens up new avenues for research. In particular, envisioning the AI Act as a source of contract regulation calls for careful consideration of its interactions with general contract law rules of Member States. On the one hand, specific attention should be paid to the existing differences among national legal systems that may lead to significantly distant outcomes depending on the place where a claim is brought. On the other hand, those same differences between the solutions consolidated within Member States' law should be assessed, on the basis of comparative studies, before proposals to harmonise rules on AI procurement contracts at the European level are advanced.
From a different perspective, and in conclusion, analysing the interplay between the AI Act and contractual agreements will be relevant to evaluate the success of the Regulation itself and of its ambition to establish uniform standards beyond the borders of the European Union. It seems reasonable to believe that the dissemination of the values it conveys will largely depend on its ability to engage with contractual practices and the ways they influence the governance of AI.

Abstract

This paper explores the role of contracts in shaping the governance of AI across the private and public sectors. It investigates, in particular, how contractual agreements between the providers and deployers of AI systems influence the level of transparency of automated decision-making and the allocation of risks and liability between the parties. It is argued that these contracts establish a regulatory framework that operates alongside, or even in the shadow of, existing legislation, potentially undermining the effectiveness of access to information rights under the GDPR and the AI Act.

Keywords

AI procurement – information duties – transparency – automated decision-making – AI explainability