PACTA SUNT SERVANDA REVISITED? TRADITIONAL LEGAL PRINCIPLES VIS-À-VIS SMART CONTRACTS UNDER THE EU DATA ACT

Tomáš Křivka

Abstract: Smart contracts, as self-executing digital agreements implemented via blockchain technology, represent an unprecedented challenge to traditional contract law doctrines, particularly the principle of *pacta sunt servanda* – the sanctity of contracts. This paper provides a comprehensive examination of smart contracts within the European legal framework, focusing on their technological nature, regulatory treatment under the EU Data Act and their compatibility with established contractual principles. The paper analyses key tensions arising from the immutable, automated nature of smart contracts, including problems related to oracles, kill switches, good faith obligations, contract modification and termination, and consumer protection. Through critical evaluation of the Article 36 requirements, this paper concludes that while the legislation represents a commendable first regulatory response, significant risks and challenges remain. The article argues that future regulation must strike a delicate balance between preserving the technological advantages of smart contracts and maintaining the flexibility, equity, and judicial oversight inherent in European contract law tradition.

Resumé: Chytré smlouvy (někdy také inteligentní smlouvy) jsou digitální dohody automaticky vykonávané prostřednictvím technologie blockchain a představují bezprecedentní výzvu pro tradiční doktríny smluvního práva, zejména pro princip *pacta sunt servanda*. Tento článek poskytuje analýzu chytrých smluv v rámci evropského právního rámce se zaměřením na jejich technologickou povahu, regulační úpravu podle nařízení EU o datech a jejich kompatibilitu s klasickými smluvními principy. Příspěvek analyzuje klíčové rozpory vyplývající z neměnné, automatizované povahy chytrých smluv, včetně problémů souvisejících s tzv. *orákuly*, *kill switchem*, závazkem dobré víry, či změnou a ukončením smluv nebo principem ochrany spotřebitele. Prostřednictvím kritického hodnocení požadavků článku 36 nařízení o datech autor dochází k závěru, že ačkoli legislativa představuje chvályhodnou první regulační snahu, nadále přetrvávají značná nevyřešená rizika a sporné otázky. Autor dokládá, že budoucí regulace musí lépe najít křehkou rovnováhu mezi zachováním technologických výhod chytrých smluv a zaručením flexibility, rovnosti a efektivního soudního dohledu tradičně garantovaných v rámci evropského smluvního práva.

Key words: Smart contracts, Blockchain, EU Data Act, Contractual Law Principles, Pacta Sunt Servanda

About the Author:

Tomáš Křivka graduated from the Faculty of Law, University of West Bohemia, Czech Republic, he also studied at School of Law, Manchester Metropolitan University in the UK. His research and academic activities are mainly focused on issues of new digital challenges within the EU legal regime and Europeanisation of private law in EU Member States. Apart from his academic career, he is a practising attorney-at-law qualified in the Czech Republic. Email: **krivka@kup.zcu.cz.**

1. Introduction: The Digital Revolution in Contract Law

The emergence of smart contracts represents one of the most profound challenges to traditional contract law doctrine in modern legal history. These self-executing digital agreements, encoded on blockchain networks and executed automatically without human intervention, fundamentally alter the landscape in which the ancient principle of *pacta sunt servanda* operates.[1] For centuries, European contract law has been built upon a delicate balance between the sanctity of agreements and the flexibility necessary to achieve justice in individual cases. The principle that agreements must be kept has never been absolute; it has always coexisted with doctrines of good faith, changed circumstances, mistake, duress, and judicial discretion to modify or terminate contracts when equity demands.[2] Smart contracts, by their very nature, threaten to upset this balance by introducing an unprecedented degree of rigidity and automation into contractual relationships. Once deployed on an immutable blockchain, code executes regardless of changed circumstances or unforeseen hardships.[3] For instance, a smart contract for international trade automatically triggers payment upon receiving shipment confirmation, regardless of whether goods arrive damaged, leaving no room for negotiation about refunds. This stands in contrast to European legal traditions recognizing contracts as complex relationships requiring ongoing interpretation and adaptation to ensure fairness.

The EU response to this challenge, embodied primarily in the EU Data Act[4] and specifically its Article 36, represents the first major legislative attempt to reconcile the promise of smart contract technology with the fundamental requirements of legal certainty, party autonomy, and consumer protection. Article 36 imposes essential requirements on smart contracts used in data- sharing contexts, mandating that such contracts include mechanisms for termination, interruption, and human control. This regulatory intervention reflects a profound recognition that pure code-based automation, without legal safeguards and human oversight, is incompatible with the values that underpin European contract law. The EU Data Act's approach suggests that even in the digital age, law must remain supreme over technology, and that the efficiency gains promised by smart contracts cannot come at the expense of justice, fairness, and the protection of fundamental rights.[5] However, the EU Data Act's limited scope (applying only to data-sharing agreements) leaves vast areas of smart contract usage unregulated, creating significant gaps in the legal framework. Moreover, the technical standards and implementation mechanisms necessary to give effect to requirements by Article 36 remain under development, leaving considerable uncertainty about how they will operate in practice.[6]

---

1 SZABO, N., 'Smart Contracts: Building Blocks for Digital Markets' (1996), reprinted in N. SZABO, 'Smart Contracts: Formalizing and Securing Relationships on Public Networks', *First Monday* 2, no. 9 (1997), available at https://doi.org/10.5210/fm.v2i9.548. Accessed 18 August 2025.

2 LANDO, O., BEALE, H. (eds.), '*Principles of European Contract Law, Parts I and II*' (Kluwer Law International, 2000) pp. 113–142.

3 WERBACH, K., CORNELL, N., 'Contracts Ex Machina' (2017) 67 *Duke Law Journal* 313, pp. 320–328.

4 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L 2023/2854.

5 PAECH, P., 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1073, pp. 1085–1092.

6 FINCK, M., 'Smart Contracts as a Form of Solely Automated Processing under the GDPR' in SCHOLZ, L. A. (ed.) *'Data Protection, Privacy and European Regulation in the Digital Age*' (Nomos, 2021), pp. 157–182.

Beyond the specific provisions of the EU Data Act, the challenge of integrating smart contracts into European law raises fundamental questions about the nature of contractual obligation, the role of judicial interpretation, and the limits of party autonomy. The jurisprudence of the Court of Justice of the European Union (hereinafter just "CJEU"), while not yet directly addressing smart contracts, provides important guidance through its decisions on automated decision-making, consumer protection in digital environments, and the interpretation of contracts in cross-border contexts.[7] Case C-203/22 (discussed in Section 5) establishes that automated decision-making systems must be subject to human oversight, suggesting purely automated smart contracts without human review may violate fundamental rights.[8] Similarly, the Court's extensive jurisprudence on consumer protection establishes that contractual terms must be transparent, fair, and subject to judicial control – requirements that sit uneasily with the technical complexity and immutability of smart contract code. Academic literature on smart contracts reveals a fundamental debate[9]: proponents emphasize efficiency gains and elimination of opportunistic breach through automation,[10] while critics warn that inflexibility sacrifices essential legal protections developed over centuries to ensure fairness.[11] This debate reflects competing visions of what contract law should be: rigid rules promoting certainty, or flexible frameworks balancing certainty with justice.[12]

2. The Technical Architecture of Smart Contracts and Its Legal Implications

To understand the legal challenges posed by smart contracts, one must first appreciate their technical architecture and how it differs fundamentally from traditional contractual arrangements. A smart contract is essentially a computer program stored on a blockchain: a distributed, decentralized ledger maintained across multiple nodes in a network.[13] When parties create a smart contract, they encode their agreement into computer code, specifying conditions that trigger automatic execution of contractual obligations. For example, a simple smart contract for the sale of goods might be programmed to release payment automatically upon verification that goods have been delivered, as confirmed by data from an Internet of Things device or oracle providing external information to the blockchain.[14] Once deployed on the blockchain, the

7 DE FILIPPI, P., WRIGHT, A., '*Blockchain and the Law: The Rule of Code*' (Harvard University Press, 2018), pp. 72–98.

8 Case C-203/22, *SCHUFA Holding AG*, EU:C:2024:495.

9 RASKIN, M., 'The Law and Legality of Smart Contracts' (2017) 1 *Georgetown Law Technology Review* 305, pp. 310–325.

10 SAVELYEV, A., 'Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law' (2017) 26 *Information, Communications Technology Law* 116, pp. 120–128.

11 SKLAROFF, J. M., 'Smart Contracts and the Cost of Inflexibility' (2017) 166 *University of Pennsylvania Law Review* 263, pp. 280–295.

12 PAŁKA, P., 'Tackling the Blockchain Governance Dilemma: On the Blockchain State and Administrative Law' in M. FINCK, M. KRITIKOS, L. MOSCON (eds.), *Blockchain and the General Data Protection Regulation* (European Parliament, 2019), pp. 35–52.

13 NAKAMOTO, S., '*Bitcoin: A Peer-to-Peer Electronic Cash System*' (2008) Available at: <https://bitcoin.org/bitcoin.pdf>. Accessed 18 August 2025.

14 WOOD, G., '*Ethereum: A Secure Decentralised Generalised Transaction Ledger*' (2014) Ethereum Project Paper 151.

smart contract operates autonomously, executing its coded instructions whenever the specified conditions are met, without requiring further action or consent from the parties.[15]

The key technical feature that creates legal challenges is the immutability of blockchain-based smart contracts. Unlike traditional contracts, which exist as text that can be interpreted, modified by mutual agreement, or set aside by courts, smart contracts consist of code that, once deployed on most blockchain networks, cannot be altered or reversed.[16] This immutability is precisely what makes blockchain technology valuable for many applications – it ensures that records cannot be tampered with and that transactions, once executed, are final. However, this same immutability creates profound problems for contract law. If parties discover an error in the code, experience a fundamental change in circumstances, mutually agree to modify their agreement, or if a court determines that the contract is illegal or unconscionable, the smart contract may nonetheless continue executing according to its original programming.[17] While technically sophisticated solutions exist (such as multi-signature mechanisms requiring multiple parties' approval before execution, time-locks that delay execution or upgradeability patterns that allow code modification under certain conditions), these solutions are not universally implemented and themselves introduce new complexities and vulnerabilities.[18]

The automated execution characteristic of smart contracts also raises fundamental questions about the nature of contractual obligation and performance. In traditional contract law, performance is a human act, subject to the performer's judgment, discretion, and good faith.[19] Contract law recognizes that parties must cooperate in performance, act reasonably to facilitate each other's performance, and sometimes adapt their conduct to changed circumstances or the counterparty's needs. Good faith requirements[20] (discussed in detail in Section 4) present significant challenges for automated execution. Smart contracts cannot incorporate good faith considerations but follow their programming automatically, regardless of whether execution would be fair or consistent with parties' intentions. [21]

Furthermore, the transparency of smart contracts is more apparent than real. While the code of a smart contract deployed on a public blockchain is theoretically visible to anyone, understanding 'what that code actually does' requires significant technical expertise in computer programming and blockchain technology.[22] For most parties, particularly consumers and small businesses, smart contract code is effectively inscrutable – a black box whose operations they

[15] See European Central Bank: Distributed Ledger Technology in Post-Trade Settlement (2016). Available at: <https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>. Accessed 18 August 2025.

[16] YEUNG, K., 'Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82 *Modern Law Review* 207, pp. 215–225.

[17] MIK, A., 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) *9 Law, Innovation and Technology* 269, pp. 280–292.

[18] AGOSTINI, L., '*Blockchain and Smart Contracts: The EU's (Lacking) Approach*' (2019) Luiss Guido Carli University, pp. 42–58.

[19] UNIDROIT Principles of International Commercial Contracts 2016, Article 1.7 (Good Faith and Fair Dealing).

[20] Principles of European Contract Law (PECL), Article 1:201 (Good Faith and Fair Dealing), in LANDO, O. et al. (eds.), '*Principles of European Contract Law*' (Kluwer, 2000).

[21] PAECH, P., 'Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty?' (2016) 21 *Uniform Law Review* 612, pp. 625–633.

[22] European Law Institute, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (2022), Principles 3.1-3.3. Available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_ Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection.pdf. Accessed 18 August 2025.

must take on faith. This information asymmetry creates serious problems for legal doctrines premised on informed consent and mutual understanding.[23] If parties cannot meaningfully understand what they are agreeing to, can their consent be considered genuine? If a consumer cannot read code but must rely on natural language explanations provided by the contract's creator, what happens when the code's actual operation diverges from those explanations? EU consumer protection law, which requires that contract terms be clear, comprehensible, and transparent, seems difficult to reconcile with the technical complexity of smart contract code.[24] The emphasis by CJEU on meaningful information and the ability of ordinary persons to understand their contractual rights suggests that purely code-based contracts, without accessible explanations and human oversight, may fail basic legitimacy tests.[25]

The global, borderless nature of blockchain technology creates additional complications for legal systems organized around territorial jurisdiction. A smart contract might be created by parties in different countries, stored on a blockchain with nodes distributed across multiple jurisdictions, and govern a transaction involving the transfer of assets located in yet another jurisdiction.[26] Which country's law governs such a contract? Which courts have jurisdiction over disputes? How can court judgments be enforced against a decentralized blockchain system with no central authority or identifiable operator? Traditional private international law rules, developed for contracts with clear connections to particular territories, struggle to accommodate the deterritorialized nature of blockchain-based transactions. The Rome I Regulation on the law applicable to contractual obligations[27] provides rules for determining governing law, but applying these rules to smart contracts raises novel questions.[28] Do smart contracts have a characteristic place of performance? Can parties effectively choose governing law when their agreement is encoded rather than written in natural language? These questions remain largely unresolved, creating significant legal uncertainty for parties using smart contracts in cross-border transactions.

3. The EU Data Act: Regulatory Innovation and Its Limits

3.1 Overview and Regulatory Context

The EU Data Act, which entered into force on January 11, 2024, but only became fully applicable from September 12, 2025, represents a watershed moment in European digital governance. This comprehensive legislative framework addresses data-driven innovation and the emerging phenomenon of smart contracts within the EU legal ecosystem. The regulation

[23] SPINDLER, G., 'Smart Contracts and Consumer Protection: Challenges and Opportunities' (2019) 10 *European Review of Private Law* 827, pp. 835–845.

[24] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/29.

[25] Case C-415/11, *Mohamed Aziz v Caixa d'Estalvis de Catalunya, Tarragona i Manresa*, EU:C:2013:164, paras 68–70.

[26] FINCK, M., MOSCON, V., 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0' (2019) 50 *International Review of Intellectual Property and Competition Law* 77, pp. 85–92.

[27] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177/6.

[28] DE HERT, P., PAPAKONSTANTINOU, V., KAMARA, I., 'The New Cloud Computing ISO/IEC 27018 Standard through the Lens of the EU Legislation on Data Protection' (2016) 32 *Computer Law, Security Review* 497, pp. 505–512.

emerged from a policy imperative recognized by EU institutions. Without clear regulatory standards, blockchain-based smart contracts would operate in a legal vacuum, creating uncertainty for businesses, inadequate protections for consumers, and competitive disadvantages for EU-based developers relative to jurisdictions offering clearer regulatory guidance.

The Data Act pursues multiple interconnected objectives: (1) facilitating equitable access to and sharing of non-personal machine-generated data; (2) preventing unfair contractual terms that inhibit data sharing or impose lock-in effects; (3) enabling portability and switching between data processors and cloud services; (4) establishing essential technical and functional requirements for smart contracts deployed within data-sharing contexts. Among these objectives, the regulation's treatment of smart contracts, codified in Article 36, represents its most technically novel and legally challenging provision. The rationale underlying Article 36 reflects a deliberate policy choice: rather than banning smart contracts or subjecting them to prohibitive requirements, the EU opted for managed regulation. The regulation presumes that smart contracts offer legitimate benefits—efficiency, reduced intermediation costs, enhanced transparency, and faster transaction processing. Yet unregulated deployment poses risks: consumers may face exploitation through opacity, counterparties may experience lock-in, and legal uncertainties may deter responsible innovation. Article 36 thus aims to establish guardrails enabling beneficial automation while protecting against demonstrable harms.

3.2 Specific Technical and Functional Requirements

Article 36(1) establishes four essential requirements applicable to "smart contracts" used for executing data-sharing agreements within the Data Act's material scope:

3.2.1 Robustness and Safety Requirements – Article 36(1)(a)

The regulation mandates that smart contracts incorporate mechanisms to prevent errors and detect anomalies. Specifically, contracts must be "designed with internal functions to prevent and monitor errors in automatic performance." This requirement acknowledges a fundamental technical reality: code contains bugs, data feeds provide inaccurate information, and external conditions may render automatic execution inappropriate. The practical implications are that developers must implement error detection mechanisms, i.e. functions that continuously monitor execution against pre-agreed parameters and alert parties or suspend execution upon detecting deviations. Examples include threshold limits on transaction values, rate-of-change sensors on oracle data, and consistency checks across multiple data sources. However, the regulation does not specify what constitutes "adequate" error prevention or detection; this ambiguity creates compliance uncertainty for developers. Mandating comprehensive error prevention across all scenarios arguably imposes impossible requirements. No software development regime guarantees the absence of all bugs. Requiring developers to implement "perfect" error detection could expose them to strict liability regimes exceeding traditional product liability standards.

3.2.2 The "Kill Switch" Provision – Article 36(1)(b)

Perhaps the Data Act's most controversial requirement, Article 36(1)(b) mandates that smart contracts provide 'a safe termination function allowing the underlying agreement to be terminated and securely resetting the state of the ledger, where this is relevant.' This provision directly confronts blockchain's central value proposition – immutability – by requiring

that parties retain the technical capacity to halt, modify, or reverse contract execution after deployment (see Chapter 2 for more details).

3.2.3 Data Access and Interoperability – Article 36(1)(c)

The regulation stipulates that smart contracts "shall not impede, restrict or prevent the exercise of rights granted" regarding data access and portability. In practical terms, smart contracts must not prevent parties from accessing data or switching to alternative service providers. This requirement addresses "lock-in" concerns. In digital markets, dominant platforms often embed switching costs through proprietary data formats, restricted APIs (application programming interfaces), or technical barriers preventing data export. By prohibiting data access impediments, Article 36(1)(c) aims to preserve competitive market conditions and party autonomy in data-sharing ecosystems. For blockchain-based smart contracts, interoperability requirements may necessitate standardized data formats, open APIs enabling third-party integration, and protocols facilitating cross-platform data transfer. However, the regulation does not specify technical standards, creating uncertainty regarding compliance.

3.2.4 Transparency and Auditability (Emphasized in Recitals)

While not formally enumerated as a separate essential requirement, the Data Act's Recitals emphasize that smart contract functioning must be "transparent, comprehensible and auditable" to contracting parties and competent authorities. This principle reflects the recognition that algorithmic opacity undermines informed consent and regulatory oversight. Transparency can be understood in more dimensions, e.g. as code accessibility (parties should be able to examine the contract's logic, ideally through source code made available in accessible programming languages), or as functionality documentation (natural language descriptions of the contract's operation, consequences of execution, and triggering conditions must be clear and accurate), or as oracle disclosure (the identity, methodology, and accuracy track record of external data feeds must be disclosed) or even as audit trails (blockchain's immutable transaction records should be maintained and made accessible for forensic analysis).

3.3 Implementation Gaps and Regulatory Uncertainty

Article 36 establishes binding requirements, yet leaves crucial implementation details unresolved, creating regulatory uncertainty in quite a few different areas such as:

3.3.1 Undefined Compliance Standards

Article 36 requires 'robustness' and 'safety' without defining precisely what constitutes adequate robustness. How many redundant data sources satisfy interoperability requirements? What accuracy rate for oracles is acceptable? How frequently must anomaly monitoring occur? The regulation provides no quantitative thresholds or technical specifications. Consequently, developers must undertake costly legal analysis to determine compliance. This creates barriers to entry for smaller firms and innovative startups, while larger enterprises with in-house legal resources more easily navigate ambiguity. The resulting regulatory burden may paradoxically disadvantage European developers relative to counterparts in jurisdictions with either stricter but clearer standards or minimal oversight.

3.3.2 Delegated Acts Absence

Article 36(3) authorizes the European Commission to adopt delegated acts specifying technical standards implementing these requirements. However, as of September 2025, the

Commission has not yet adopted such acts. This delay reflects the genuine technical complexity of translating legal requirements into implementable technical standards. Meanwhile, smart contract developers operate under provisional compliance frameworks rather than definitive standards. Until delegated acts are adopted, developers cannot rely on Commission guidance to determine compliance with reasonable certainty.

3.3.3 Oracle Governance Vacuum

While Article 36 references data accuracy, the regulation does not establish detailed oracle governance frameworks. Three critical dimensions remain unaddressed: First, the regulation establishes no clear liability standards for oracle operators providing erroneous data. Second, the regulation does not specify GDPR compliance mechanisms for oracle data processing. Third, the regulation lacks mandatory certification or quality assurance schemes for oracle providers or mandatory redundancy or multi-source verification requirements. Without clear oracle governance standards, market participants cannot meaningfully assess oracle reliability or enforce accountability when oracles malfunction. The EU has effectively delegated oracle governance to private market actors, providing minimal regulatory guidance. This creates information asymmetries that undermine informed contracting and introduces systemic risks that could propagate across data-sharing ecosystems relying on common oracle infrastructure.

3.3.4 Enforcement Mechanism Ambiguity

The Data Act assigns enforcement to national competent authorities. However, on blockchain networks, identifying and sanctioning non-compliant smart contracts proves technically challenging. Smart contracts are deployed through pseudonymous addresses; they execute on distributed networks spanning multiple jurisdictions; and identifying the 'responsible party' for non-compliance becomes legally complex. Traditional enforcement mechanisms (inspections, warning notices, escalating penalties) presume identifiable regulated entities. Smart contracts complicate this assumption. How do national authorities even identify that a particular smart contract violates Article 36? How do they isolate the developer, deployer, or platform operator responsible? How do they serve enforcement notices on pseudonymous actors? Until these procedural questions are resolved, Article 36's substantive requirements may prove unenforceable in practice.

3.4 Jurisdictional and Territorial Application Issues

Article 36 applies to smart contracts involving EU data holders or recipients, regardless of where the blockchain infrastructure is physically located. This extraterritorial application creates several complications, which we will discuss below.

3.4.1 Cross-jurisdictional conflicts

Consider a smart contract deployed on Ethereum (a globally distributed network) executed between a German manufacturer (EU-based) and a Singapore supplier (non-EU). Article 36 technically applies because an EU party is involved. Yet the Singapore party operates under different legal regimes; Singapore law may not recognize mandatory kill switch requirements or may impose conflicting obligations. How should parties comply simultaneously with EU and Singapore law?

3.4.2 Forum and choice of law complexity

Regulation (EC) 593/2008 (Rome I) governs choice of law for contractual obligations. Smart contracts complicate application of Rome I principles: Which "law" governs when performance is automated and instantaneous? If the code itself is the contract, and code is law-neutral, how do conflict rules apply? When parties are pseudonymous, Rome I's mechanisms for discerning intent regarding choice of law fail.

3.4.3 Pre-Existing Smart Contracts

Article 36 applies to smart contracts deployed after the Data Act's application date, while pre-existing smart contracts remain unregulated, creating a legacy population of non-compliant contracts that will continue operating indefinitely. This temporal gap creates both competitive disadvantages for compliant new entrants and regulatory arbitrage incentives for parties preferring pre-Data Act frameworks.

3.4.4 Scope Limitation to Data-Sharing Contexts

Article 36 explicitly applies only to smart contracts deployed within data-sharing contexts governed by the Data Act. Other smart contract applications (e.g. financial derivatives, supply chain management, identity verification systems) remain outside Article 36's scope. This selective application creates regulatory classification challenges: when does a smart contract constitute a "data-sharing agreement" triggering Article 36 obligations versus a commercial contract outside the regulation's scope?

3.5 Penalties and Enforcement Provisions

Article 41 of the Data Act establishes that Member States shall prescribe rules on penalties for infringements, including violations of Article 36 requirements. Penalties must be "effective, proportionate and dissuasive." However, the Data Act does not specify a few key features or issues regarding the penalties. A primary unresolved issue concerns penalty magnitude. Should Article 36 violations incur: (a) the 2% global turnover model applicable to GDPR breaches; (b) scaled percentages based on contract value; or (c) fixed administrative fines per violation? Also, it is unclear how liability should be allocated. If a smart contract violates Article 36, should liability attach to the developer, the deployer, the platform operator, or some combination? Significant troubles also arise in term of enforcement procedures: how do national authorities identify violations on distributed, pseudonymous networks? Another unsolved issue remains in the cooperation mechanisms: When smart contracts span multiple EU Member States, how do regulators coordinate enforcement? All these ambiguities create enforcement uncertainty since regulated parties cannot reliably predict compliance costs or penalty exposure.

3.6 Substantive Deficiencies of Article 36

3.6.1 Good Faith and Equitable Considerations

While Article 36 mandates "transparency," it does not require smart contracts to incorporate mechanisms ensuring good faith performance or equitable outcomes in exceptional circumstances. Smart contracts satisfying technical requirements according to Article 36 could still mechanically enforce terms in ways that violate fundamental good faith principles recognized in European contract law.

3.6.2 Hardship and Force Majeure

Traditional European contract law recognizes doctrines of hardship and force majeure, permitting contract modification or termination when unforeseen events render performance excessively burdensome or impossible. Kill switches provide partial remedy but leave gaps. Article 36 does not mandate that parties include hardship or force majeure triggers in their kill switch provisions; termination might be available only for fraud or illegality, not for supervening economic impossibility.

3.6.3 Consumer Remedies Beyond Termination

While Article 36 envisions consumer protection through kill switches and transparency, it does not comprehensively address consumer remedies for defective smart contract performance. If a smart contract executes incorrectly due to oracle error or code bug, can consumers obtain damages? Replacement? Repair? EU consumer protection law normally guarantees such remedies; Article 36 does not explicitly preserve them in smart contract contexts.

4. Pacta Sunt Servanda and the Principles of European Contract Law

To understand the challenge that smart contracts pose to European contract law, one must appreciate the leading role of *pacta sunt servanda* and its relationship to other fundamental principles. *Pacta sunt servanda* – the principle that agreements must be kept – is perhaps the most fundamental norm of contract law, appearing in virtually every legal system and recognized as a general principle of international law.[29] The principle reflects the basic moral and practical necessity of keeping promises: social cooperation, commercial exchange, and economic planning all depend on the ability of parties to rely on each other's commitments. Without a strong norm of promise-keeping, contract law could not fulfil its essential functions of facilitating exchange, allocating risk, and enabling parties to plan the future with confidence.[30]

However, *pacta sunt servanda* has never been absolute. Throughout the history of European contract law, the principle has been balanced by numerous exceptions and limitations that permit parties to escape or modify their obligations under certain circumstances.[31] The doctrine of impossibility excuses performance when unforeseen events make performance objectively impossible. The doctrine of frustration or force majeure excuses performance when changed circumstances fundamentally alter the nature of the contractual obligation, making performance radically different from what was originally contemplated.[32] The doctrine of hardship, recognized in many civil law systems and in international instruments like the UNIDROIT Principles, permits contract adaptation or termination when changed circumstances make performance excessively onerous for one party, disrupting the equilibrium of the contract.[33] The doctrine of mistake allows contracts to be set aside when parties labour under fundamental misunderstandings about material

[29] Vienna Convention on the Law of Treaties 1969, Article 26 (Pacta sunt servanda).

[30] KÖTZ, H., FLESSNER, A., *European Contract Law* (Oxford University Press, 1997), pp. 11–15.

[31] ZIMMERMANN, R., *The Law of Obligations: Roman Foundations of the Civilian Tradition* (Oxford University Press, 1996), pp. 580–620.

[32] CARTWRIGHT, J., HESSELINK, M. (eds.), *Precontractual Liability in European Private Law* (Cambridge University Press, 2008), pp. 189–210.

[33] UNIDROIT Principles 2016, Articles 6.2.1–6.2.3 (Hardship).

facts. The doctrine of unconscionability permits courts to refuse enforcement of contracts or contract terms that are grossly unfair or oppressive.[34]

Beyond these specific doctrines, European contract law is permeated by the principle of good faith and fair dealing. The Principles of European Contract Law state in Article 1:201 that each party must act in accordance with good faith and fair dealing. This principle requires parties to act honestly, to cooperate in performing their obligations, to refrain from taking advantage of the other party's vulnerabilities or mistakes, and to consider the legitimate interests of the counterparty. Good faith obligations extend throughout the contract lifecycle – in negotiation, performance, and enforcement.[35] A party may not stand on strict legal rights when doing so would violate good faith, may not exploit ambiguities or technical loopholes to escape obligations or impose unexpected burdens, and may not refuse to renegotiate or adapt the contract when changed circumstances make such adaptation reasonable.[36]

The flexibility inherent in these doctrines and principles serves essential purposes. Contracts are necessarily incomplete – parties cannot foresee and provide for every possible contingency.[37] The world changes in unexpected ways, and circumstances that seemed reasonable at contract formation may later prove impossible or profoundly unjust. Parties sometimes make mistakes, may be unequally sophisticated or powerful, and may need protection against exploitation. Rigid enforcement of contracts without regard to these realities would frequently produce unjust results, undermine the social legitimacy of contract law, and ultimately reduce parties' willingness to enter contracts in the first place.[38] The flexibility provided by good faith, changed circumstances doctrines, and judicial oversight ensures that contract law remains aligned with its underlying purposes of facilitating cooperation and exchange while preventing oppression and exploitation.

Smart contracts, however, threaten to eliminate this flexibility. By encoding obligations in computer code and executing them automatically, smart contracts remove the human discretion and contextual judgment that have always been central to contract performance and enforcement.[39] A smart contract cannot assess whether performance has become impossible or whether circumstances have changed so fundamentally that performance should be excused. It cannot recognize mistakes or misunderstandings. It cannot apply good faith principles to determine whether insisting on performance would be unconscionable. It simply executes its code according to strict logical rules, without regard to context, consequences, or fairness.[40] In this sense, smart contracts threaten to implement *pacta sunt*

[34] TEUBNER, G., 'Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergences' (1998) 61 *Modern Law Review* 11, pp. 20–28.

[35] WHITTAKER, S., ZIMMERMANN, R., 'Good Faith in European Contract Law: Surveying the Legal Landscape' in R. ZIMMERMANN, S. WHITTAKER (eds.), *Good Faith in European Contract Law* (Cambridge University Press, 2000), pp. 7–62.

[36] BROWNSWORD, R., 'Freedom of Contract, Human Rights and Human Dignity' in D. FRIEDMANN, D. BARAK-EREZ (eds.), *Human Rights in Private Law* (Hart Publishing, 2001), pp. 181–199.

[37] AYRES, I., GERTNER, R., 'Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules' (1989) 99 *Yale Law Journal* 87, pp. 91–115.

[38] EISENBERG, M., 'The Responsive Model of Contract Law' (1984) 36 *Stanford Law Review* 1107, pp. 1120–1135.

[39] LESSIG, L., *Code and Other Laws of Cyberspace* (Basic Books, 1999), pp. 85–99.

[40] MÖSLEIN, F., OMLOR, S., 'Private Law and Blockchain Technology: Comparative Approaches' in M. FINCK et al. (eds.), *Blockchain and the Law* (Edward Elgar, 2021), pp. 203–228.

servanda in an extreme, uncompromising form – not the balanced principle of traditional contract law, but an absolutist version that brooks no exceptions.

Some scholars and blockchain advocates view this as a virtue rather than a vice. They argue that contract law's flexibility is actually a weakness, creating uncertainty and enabling opportunistic breach.[41] If parties know that they may be able to escape obligations by claiming changed circumstances, mistake, or good faith defences, they have less incentive to perform and more incentive to search for excuses. Smart contracts, by eliminating these escape routes, create stronger incentives for performance and more reliable enforcement. From this perspective, smart contracts represent a valuable innovation that solves the perennial problem of opportunistic breach and returns contract law to its fundamental purpose of enforcing promises.[42] The immutability and automation of smart contracts, rather than being flaws, are features that make contracts more credible and valuable.

However, this perspective overlooks crucial problems. First, it assumes that parties can foresee all relevant contingencies and encode appropriate responses in their smart contracts. Parties are boundedly rational, the future is uncertain, and many contingencies that will prove important cannot be anticipated.[43] A rigid system that provides no flexibility to respond to genuinely unforeseen circumstances will frequently produce inefficient and unjust results. Second, the argument assumes that the problem of opportunistic breach is more significant than the problem of opportunistic insistence on performance. Parties may act opportunistically by demanding performance when circumstances have changed so dramatically that performance no longer serves the contract's underlying purposes.[44] Flexibility protects against both opportunistic breach and opportunistic insistence on performance. Third, the argument ignores information asymmetries and power imbalances between parties. In consumer contracts and contracts between parties of unequal sophistication or bargaining power, the weaker party often cannot meaningfully negotiate terms or fully understand what they are agreeing to.[45] Judicial oversight and mandatory rules protecting weaker parties are essential for preventing exploitation. Smart contracts that execute automatically, without such oversight, risk enabling rather than preventing injustice.

5. The Jurisprudence of the CJEU

While the CJEU has not yet directly addressed smart contracts in its case law, its jurisprudence on related issues provides important guidance for understanding how European law is likely to approach smart contract challenges. Several lines of CJEU case law are particularly relevant: decisions concerning automated decision-making under the General Data Protection Regulation, rulings on consumer protection in digital environments, and the Court's general approach to contract interpretation and party autonomy.[46] The decision

41 SWAN, A., '*Blockchain: Blueprint for a New Economy*' (O'Reilly Media, 2015), pp. 58-72.

42 BUTERIN, V., '*DAOs, DACs, DAs and More: An Incomplete Terminology Guide*' (2014) Availabe at: <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide>. Accessed on 15 August 2025.

43 HART, O., MOORE, J., 'Incomplete Contracts and Renegotiation' (1988) 56 *Econometrica* 755, pp. 760-775.

44 MACNEIL, I., 'Contracts: Adjustment of Long-Term Economic Relations Under Classical, Neoclassical, and Relational Contract Law' (1978) 72 *Northwestern University Law Review* 854, pp. 880-895.

45 COLLINS, H., *Regulating Contracts* (Oxford University Press, 1999), pp. 234-260.

46 EBERS, M., 'Regulating AI and Robotics: Ethical and Legal Challenges' in M. EBERS, S. NAVAS (eds.), *Algorithms and Law* (Cambridge University Press, 2020), pp. 37-73.

in Case C-203/22 represents the most directly relevant precedent. The case concerned automated credit scoring systems that make decisions about individuals' creditworthiness using algorithms, and specifically addressed Article 22 of the GDPR, which provides data subjects with rights regarding automated individual decision-making.[47] The Court held that Article 22 grants data subjects the right not to be subject to decisions based solely on automated processing that produce legal effects or similarly significantly affect them, unless certain conditions are met. Even where automated decision-making is permissible, data subjects have rights to obtain meaningful information about the logic involved, to express their point of view, and to contest the decision.[48] The Court emphasized that these rights are essential for protecting individuals' autonomy and dignity in an era of increasing algorithmic decision-making.

Case C-203/22 establishes binding precedent that GDPR Article 22's requirement for human oversight applies directly to smart contracts. This means EU courts will likely invalidate purely automated smart contracts that execute without meaningful human review or contestation rights. Many smart contracts make decisions that significantly affect parties – determining whether payments are made, whether goods are delivered, whether penalties are imposed.[49] If these decisions are made through purely automated processing, without meaningful human review or the possibility of contestation, they may violate the principles established by the Court. The case suggests that even technologically sophisticated automated systems must preserve space for human judgment, explanation, and challenge.[50] Applied to smart contracts, this would seem to require mechanisms for parties to understand how the code makes decisions, to challenge outcomes they believe are incorrect or unjust, and potentially to obtain human review of automated decisions. This sits uneasily with the trustless ideal of blockchain systems, where the entire point is to eliminate the need for human intermediaries or trust in third parties.[51]

However, the implications of Case C-203/22 for smart contracts extend beyond formal GDPR compliance. The Court's reasoning establishes that Article 22 GDPR protections cannot be circumvented through technical means. If a smart contract makes decisions significantly affecting parties' rights, the automated decision-making safeguards of Article 22 apply regardless of whether the decision-making occurs through traditional algorithmic systems or through code deployed on a blockchain. This establishes important jurisprudential foundation: neither decentralization nor immutability of the underlying technology creates exemption from mandatory human rights protections. The judgment moreover suggests that meaningful human oversight cannot be relegated to post-execution review; Article 22 requires contestation rights and meaningful information before execution occurs. Applied to smart contracts, this creates practical tension: blockchains operate on principle of finality (transactions cannot easily be reversed), yet Article 22 implies right to prior human review.

47 Case C-203/22, *SCHUFA Holding AG*, EU:C:2024:495, paras 45-52.

48 Ibid, paras 58–63.

49 VEALE, M., EDWARDS, L., 'Clarity, Surprises, and Further Questions in the Article 22 GDPR Order on Automated Decision-Making and Profiling' (2018) 34 *Computer Law, Security Review* 398, pp. 405–412.

50 WACHTER, S., MITTELSTADT, B., FLORIDI, L., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76, pp. 82–88.

51 DE FILIPPI, D., HASSAN, S., '*Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*' (2016) 21 First Monday.

Resolving this tension requires either: (1) implementation of approval mechanisms that delay smart contract execution pending human review, or (2) comprehensive off-chain dispute resolution that permits ex post reversal of incorrect executions, even on immutable blockchains.[52]

The CJEU's extensive consumer protection jurisprudence also provides relevant guidance. In Case C-40/08, the Court held that national courts must examine *ex officio* whether arbitration clauses in consumer contracts are unfair under the Unfair Contract Terms Directive.[53] The Court reasoned that consumer protection rules are matters of public policy of such fundamental importance that courts must ensure their application regardless of the parties' procedural choices. Similarly, in Case C-168/05, the Court ruled that consumers' rights under the Unfair Contract Terms Directive cannot be waived, even through arbitration agreements.[54] These decisions establish that consumer protection in the EU is not merely a matter of private rights that parties can freely negotiate, but rather involves mandatory rules that courts must enforce to protect the weaker party.

Applied to smart contracts, this jurisprudence suggests severe limitations on pure code-based automation in consumer contexts. If a smart contract includes terms that would be unfair under the Unfair Contract Terms Directive – for example, terms allowing unilateral modification, imposing disproportionate penalties, or limiting liability – courts must be able to review and potentially invalidate those terms, regardless of whether they are encoded in computer code.[55] Moreover, the requirement that courts examine fairness ex officio implies that smart contracts cannot prevent judicial review simply by executing automatically before disputes can reach courts. The fact that a smart contract has already executed according to its code cannot preclude courts from subsequently determining that the contract was unenforceable and ordering remedies.[56] This creates significant practical problems – once a blockchain transaction is complete, reversal may be technically impossible or extremely difficult – but the legal principle seems clear: technology cannot override fundamental consumer protection rights.

The approach by CJEU to contract interpretation also has implications for smart contracts. European private international law, as codified in the Rome I Regulation, provides rules for determining which national law governs international contracts. The CJEU has interpreted these rules to emphasize party autonomy while also protecting weaker parties and ensuring that contracts are interpreted according to objective standards. In cases involving contract interpretation, the Court has emphasized that contracts should be understood according to their objective meaning as apparent to reasonable persons in the parties' position, taking account of the contract's purpose, context, and the parties' relationship.[57] Ambiguities in consumer contracts are generally interpreted *contra proferentem* – against the drafter and in favour of the consumer.

---

52 See EDPB Guidelines 05/2022 on automated individual decision-making. Available at: <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>. Accessed 18 August 2025.

53 Case C-40/08, *Asturcom Telecomunicaciones SL*, EU:C:2009:615, paras 52-59.

54 Case C-168/05, *Mostaza Claro*, EU:C:2006:675, paras 36-39.

55 REICH, N., 'More Clarity after Quelle? Electronic Means and Unfair Contract Terms in Consumer Contracts' (2010) 6 *European Review of Contract Law* 1, pp. 8-15.

56 MAK, V., 'The Consumer's Right to Transparency: What Does it Mean and How Can it be Protected?' (2019) 8 *Journal of European Consumer and Market Law* 3, pp. 6-10.

57 Case C-133/08, *Intercontainer Interfrigo SC v Balkenende Oosthuizen BV*, EU:C:2009:687, paras 42-47.

How should these interpretation principles apply to smart contracts? When the code's operation diverges from the parties' documented intentions or from natural language descriptions provided to parties, which should prevail?[58] Blockchain advocates often argue that code is law – the contract is whatever the code does, regardless of parties' subjective intentions or descriptions. However, this approach is difficult to reconcile with European contract law's emphasis on the parties' actual agreement and the objective meaning of their expressions.[59] If a consumer is told that a smart contract will operate in a particular way, but the code actually operates differently, European law would likely hold that the consumer's reasonable understanding should prevail, even if this requires courts to override the code's operation. This creates a dualist approach where the legal contract and the code implementation are distinct, and the legal contract governs when they conflict – but enforcing this distinction against an immutable blockchain poses significant practical challenges.[60]

6. Good Faith, Adaptation and Changed Circumstances in Smart Contracts

6.1 The Principle of Good Faith

The principle of good faith represents one of the most profound challenges to smart contract automation. As discussed earlier, good faith requires parties to act honestly, cooperate, and consider each other's legitimate interests throughout the contract relationship. This is not merely a subjective moral obligation but a legal requirement that courts enforce. Parties who violate good faith may be denied enforcement of contract terms, required to adapt their conduct, or held liable for damages. Good faith obligations operate at all stages: in pre-contractual negotiations, where parties must disclose material information and not mislead; in contract performance, where parties must cooperate and not obstruct the other's performance; and in contract enforcement, where parties must not abuse their rights or exploit technical advantages.[61]

Smart contracts, executing automatically according to code logic, cannot inherently incorporate good faith considerations. Consider a simple example: a smart contract for the sale of goods programs payment to release automatically upon verification that goods have been shipped.[62] The seller ships the goods, but they arrive damaged. Traditional contract law would allow the buyer to withhold payment or demand price reduction based on the breach and would require parties to cooperate to resolve the situation. The seller might offer to repair or replace the goods; the buyer might agree to accept a discount rather than pursue full remedies. These adaptive, cooperative responses embody good faith. A smart contract, however, might release payment automatically based solely on the technical confirmation of

[58] CLIVE, J., 'The Law Applicable to Transfer of Title in Global Markets and the Future of Article 8(2) Rome I' in J. BASEDOW et al. (eds.), *Encyclopedia of Private International Law* (Edward Elgar, 2017), pp. 1654–1662.

[59] SEIN, K., 'The Exercise of the Right of Withdrawal and the Obligations to Inform' in G. HOWELLS et al. (eds.), *European Consumer Law* (Ashgate, 2017), pp. 287–310.

[60] STAUDENMAYER, A., 'The Directive on the Sale of Consumer Goods and Associated Guarantees – A Milestone in the European Consumer and Private Law' (2000) 8 *European Review of Private Law* 547, pp. 555–565.

[61] WHITTAKER, S., '*Good Faith, Implied Terms and Commercial Contracts*' (2013) 129 Law Quarterly Review 463, pp. 470–480.

[62] BRIDGE, M., 'Good Faith in Commercial Contracts' in R. BROWNSWORD et al. (eds.), *Good Faith in Contract: Concept and Context* (Ashgate, 1999), pp. 139–162.

shipment, without considering the goods' condition. The buyer would then need to pursue separate legal action to recover damages – a more costly, adversarial process. The system has become more rigid and less capable of achieving equitable resolutions.[63]

More fundamentally, good faith limits how parties can exercise their contractual rights. Even if a contract's text gives one party broad discretion or apparently absolute rights, good faith requires that these rights be exercised reasonably and not in a way that unfairly prejudices the other party.[64] For instance, if a contract gives one party discretion to determine specifications, good faith requires that this discretion be exercised reasonably and consistently with the contract's purposes, not arbitrarily or opportunistically. Similarly, if circumstances change in ways that make performance significantly more burdensome for one party, good faith may require the advantaged party to agree to reasonable modifications rather than insisting on strict performance that would cause disproportionate harm.[65] Smart contracts, encoded with specific conditions and executing automatically, cannot make these nuanced, context-sensitive judgments. They follow their programming regardless of whether doing so comports with good faith.

6.2 Adaptation and Changed Circumstances

The problem of changed circumstances – addressed by doctrines of force majeure, frustration, and hardship – presents similar challenges.[66] These doctrines recognize that contracts are made against a background of assumptions about future circumstances, and that when these assumptions prove fundamentally wrong, rigid enforcement may produce unjust results.[67] The UNIDROIT Principles address this in Articles 6.2.1 through 6.2.3 on hardship. Under these provisions, hardship occurs when events fundamentally alter the equilibrium of the contract, making performance excessively onerous for one party. When hardship exists, the disadvantaged party can request renegotiation, and if renegotiation fails, either party can request that a court adapt the contract or terminate it. This framework recognizes that changed circumstances sometimes require adaptive responses but structures these responses to minimize opportunism and preserve contracts where possible.[68] The COVID-19 pandemic illustrated this: business closures, supply disruptions, and demand changes rendered many contracts impossible or pointless to perform. Traditional law responded with flexibility.[69] Smart contracts absent such mechanisms would be executed regardless, potentially requiring impossible or pointless performance.

Some argue that parties can address these problems through careful contract design, encoding appropriate responses to foreseeable contingencies. For instance, a smart contract might include conditions that excuse performance if certain objective indicators (such as

63 TWIGG-FLESNER, C., *The Europeanisation of Contract Law* (2nd ed., Routledge-Cavendish, 2013), pp. 145–168.

64 BEALE, H. (ed.), *Chitty on Contracts* (33rd ed. Sweet & Maxwell, 2018), paras 1-039 to 1-045.

65 CARTWRIGHT, J., 'The Duty to Perform in Good Faith in English Law' (2012) 16 *Edinburgh Law Review* 283, pp. 290–298.

66 DI MATTEO, L., 'Force Majeure in the Age of Climate Change and Pandemics: Lessons from CISG and the UNIDROIT Principles' (2021) 26 *Uniform Law Review* 658, pp. 670–685.

67 MCKENDRICK, E., 'Force Majeure and Frustration – Their Relationship and a Comparative Assessment' in E. MCKENDRICK (ed.), *Force Majeure and Frustration of Contract* (2nd ed., Lloyd's of London Press, 1995), pp. 31–56.

68 VOGENAUER, S. (ed.), *Commentary on the UNIDROIT Principles of International Commercial Contracts (PICC)* (2nd ed., Oxford University Press, 2015), pp. 842–875.

69 SMITS, J., 'The Principles of European Contract Law and the Harmonisation of Private Law in Europe' in A. HARTKAMP et al. (eds.), *Towards a European Civil Code* (4th ed., Kluwer, 2011), pp. 279–301.

government-declared emergencies, price indices, or supply availability) exceed specified thresholds.[70] Oracle systems could provide external data about real-world conditions, allowing smart contracts to adapt their execution accordingly. While such solutions are technically possible, they have significant limitations. First, parties cannot foresee all relevant contingencies – the very purpose of doctrines like hardship and force majeure is to address truly unforeseen events that parties could not have anticipated.[71] Second, encoding appropriate responses requires translating complex, context-sensitive legal standards into binary code logic – a task fraught with difficulty and likely to produce either over- or under-inclusive rules. Third, reliance on oracles introduces other problems of reliability, manipulation, and trust, potentially undermining the very benefits that blockchain technology promises.[72]

Moreover, even technically sophisticated flexibility mechanisms cannot fully replicate the adaptive, judgment-based approach of traditional contract law. Courts applying hardship or good faith doctrines engage in holistic, contextual analysis, considering the parties' relationship, the contract's purposes, the nature and probability of the changed circumstances, the degree of burden on each party, and the feasibility of various adaptive solutions.[73] This type of analysis requires human judgment and cannot be reduced to algorithmic rules without significant loss of nuance and responsiveness. Thus, while technical solutions can mitigate some problems, they cannot eliminate the fundamental tension between smart contract automation and the flexible, equitable approach that has characterized European contract law for centuries.[74]

Recent scholarship by IT law scholars has emphasized that the flexibility-rigidity dichotomy may be overstated. Sophisticated smart contract design patterns (including upgradeability mechanisms, circuit breakers triggered by oracle anomalies, and multi-signature approval structures) increasingly permit contextual responses to changed circumstances.[75] However, these solutions present their own legal complications: upgradeability mechanisms risk violating immutability assumptions that underlie blockchain security; oracle-triggered circuit breakers introduce new points of failure and centralized control; multi-signature requirements often concentrate decision-making among small groups of developers, undermining decentralization ideals. Thus, while technical solutions mitigate rather than eliminate the flexibility-rigidity tension, they do so by introducing new governance and security challenges that current EU regulation does not adequately address."

---

70 WERBACH, K., *The Blockchain and the New Architecture of Trust* (MIT Press, 2018), pp. 112–135.

71 BROWNSWORD, R., 'After Autonomy: Contract Relevance without Contract Validity?' in R. BROWNSWORD et al. (eds.), *The Foundations of European Private Law* (Hart Publishing, 2011), pp. 429–456.

72 XU, L. et al., 'A Taxonomy of Blockchain-Based Systems for Architecture Design' in *2017 IEEE International Conference on Software Architecture* (IEEE, 2017), pp. 243–252.

73 HONDIUS, E., SIEDEL, H., 'Good Faith and Fault in Contract Law: A Comparative Study' in E. HONDIUS (ed.), *Unexplored Aspects of the Dutch Civil Code* (Kluwer, 1996), pp. 129–152.

74 HESSELINK, M., 'The Concept of Good Faith' in A. HARTKAMP et al. (eds.), *Towards a European Civil Code* (4th ed., Kluwer, 2011), pp. 619–649.

75 SAVELYEV, A., 'Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law' (2017) 26 *Information, Communications Technology Law* 116, pp. 120–128. Also WERBACH, K., *The Blockchain and the New Architecture of Trust* (MIT Press, 2018), pp. 112–135.

7. Conclusion

Smart contracts pose profound challenges requiring reconciliation of automation efficiency with legal flexibility and fairness.[76] *Pacta sunt servanda* remains essential, not as absolute enforcement but as one principle among many oriented towards justice and cooperation.[77] Properly designed and regulated, smart contracts can reduce transaction costs and enhance transparency.[78] Yet realizing these benefits requires embedding flexibility mechanisms into design, establishing regulatory protections, creating specialized dispute resolution, and fostering legal-technical dialogue.[79]

7.1 Existing Regulation and Case-law

The EU Data Act represents an important first step, but only a first one. Comprehensive regulation of smart contracts will require extending Article 36's essential requirements to all contexts where contracts significantly affect parties' rights, developing detailed technical standards for compliance, establishing clear liability and enforcement mechanisms, and harmonizing approaches across borders to facilitate international transactions.[80] Beyond regulation, achieving legally compliant smart contracts will require technical innovation to create design patterns that accommodate legal requirements, professional education to develop interdisciplinary expertise, and cultural shifts in both legal and technical communities toward recognizing the necessity of mutual adaptation.[81] The jurisprudence of the CJEU, while not yet directly addressing smart contracts, also provides important guideposts. The Court's emphasis on human oversight of automated systems, mandatory protection for consumers and weaker parties, and the primacy of parties' actual agreement over technical implementation suggests that European law will not permit pure code-based automation to override fundamental legal protections.[82] Smart contracts will need to preserve access to courts, enable judicial review of fairness and validity, accommodate good faith obligations, and maintain the flexibility necessary to respond to changed circumstances and unforeseen events.[83]

7.2 Future Outlook

Looking forward, the successful integration of smart contracts into European contract law will serve as a test of law's adaptability in the digital age. Can legal systems previously being developed for a world of paper and human judgment successfully govern a world of

[76] BEATSON, J., FRIEDMANN, D. (eds.), *Good Faith and Fault in Contract Law* (Oxford University Press, 1995), pp. 3–28.

[77] LANDO, O., 'Some Features of the Law of Contract in the Third Millennium' (2000) 40 *Scandinavian Studies in Law* 343, pp. 350–365.

[78] UNDERWOOD, S., 'Blockchain Beyond Bitcoin' (2016) 59 *Communications of the ACM* 15, pp. 16–17.

[79] FINCK, M., *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 2019), pp. 214–238.

[80] EUROPEAN COMMISSION, 'Communication on the Digital Finance Strategy for the EU', COM (2020) 591 final.

[81] WALCH, A., 'Deconstructing Decentralization: Exploring the Core Claim of Crypto Systems' in C. BRUMMER (ed.), *Crypto Assets: Legal and Monetary Perspectives* (Oxford University Press 2019), pp. 39-68.

[82] DE BÚRCA, G., SCOTT, J. (eds.), *The EU and the WTO: Legal and Constitutional Issues* (Hart Publishing, 2001), pp. 215–240.

[83] LENAERTS, K., 'The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice' (2010) 59 *International and Comparative Law Quarterly* 255, pp. 270–285.

code and algorithmic execution?[84] Can traditional principles developed over centuries remain relevant and effective in radically new technological contexts? The answer must be yes – not because law is static and immutable, but because the values it embodies are enduring. Fairness, autonomy, cooperation, and justice remain essential regardless of the technological medium through which contracts are expressed and performed.[85] *Pacta sunt servanda* endures not as a command to enforce code blindly, but as a commitment to honour genuine, meaningful agreements – a commitment that must be revisited and renewed for each technological age but never abandoned.[86]

7.3 Recommendations De Lege Ferenda

On a more practical note, following my previous analysis in this paper, I have concluded these legislative recommendations *de lege ferenda* which could help to solve the existing gaps in the existing legal regulation of smart contracts under the EU Data Act:

a) To amend Article 36 so that it applies beyond data-sharing contexts,
b) To establish a mandatory certification framework, which would clearly distinguish between several types of smart contracts, this could work for example as follows:
Level 1: Consumer-facing contracts (max strictness),
Level 2: B2B between sophisticated parties (less strict rules),
Level 3: Experimental/research applications (relaxed rules),
c) To create an EU-wide dispute resolution mechanism for smart contracts, preferably in the form of specialized blockchain arbitration tribunals with fast-track procedures and mandatory technical experts' involvement.

[84] HILDEBRANDT, M., *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar, 2015), pp. 187–210.
[85] BROWNSWORD, M., *Rights, Regulation, and the Technological Revolution* (Oxford University Press, 2008), pp. 289–315.
[86] KELSEN, H., *Pure Theory of Law* (University of California Press, 1967), pp. 193–205.