2025 | 2

ELFR

EUROPEAN LAW AND FINANCE REVIEW

Rivista Semestrale
(Giugno/Dicembre
2025)

ISSN: 2975-0911

La sede della Redazione è presso l'Università San Raffaele di Roma,
Via di Val Cannuta n. 247, Roma, 00166

www.europeanlawandfinancereview.com

REGOLE PER LA VALUTAZIONE DEI CONTRIBUTI

Al fine di assicurare uno *standard* elevato della qualità scientifica dei contributi pubblicati, nel rispetto dei principi di integrità della ricerca scientifica, la Rivista adotta un modello di revisione dei manoscritti proposti per la pubblicazione che contempla il referaggio tra pari a doppio cieco (*double blind peer review*).

I contributi inviati alla Rivista sono oggetto di esame da parte due valutatori individuati all'interno di un elenco, periodicamente aggiornato, di Professori ordinari, associati e ricercatori in materie giuridiche.

Per ulteriori informazioni relative alla procedura di valutazione, si rinvia al Codice Etico pubblicato sul sito della Rivista.

EMAIL

info@europeanlawandfinancereview.com

REGTECH AND SUPTECH: A PROPOSAL FOR BLOCKCHAIN-CERTIFIED COMPUTATIONAL REGULATION

MICHELA PASSALACQUA

TAMARA FAVARO

RegTech and SupTech: A Proposal for Blockchain-Certified Computational Regulation*

(RegTech e SupTech: proposta di una regolazione computazionale certificata da blockchain)

Michela Passalacqua**

Full Professor of Economic Law at the University of Pisa – Department of Law

Tamara Favaro**

Associate Professor of Economic Law at the University of Pisa – Department of Law

ABSTRACT [En]:

The article analyses how RegTech and SupTech are transforming regulation and supervision in financial markets. The research proposes the use of blockchain as an infrastructure for meta-supervision, capable of ensuring traceability, verifiability and accountability of regulatory algorithms. Through an analysis of the DORA and eIDAS 2.0 Regulations, the contribution shows how Distributed Ledger Technologies can strengthen digital resilience and computational trust. The study outlines a possible new model of digital legitimation of automated public power.

Keywords: RegTech, SupTech, transparency, Distributed Ledger Technology (DLT), cybersecurity.

ABSTRACT [It]:

Il saggio analizza come RegTech e SupTech stiano trasformando la regolazione e la vigilanza dei mercati finanziari. La ricerca propone di utilizzare *blockchain* come infrastruttura di meta-vigilanza, idonea a garantire tracciabilità, verificabilità e *accountability* degli algoritmi regolatori. Attraverso l'analisi dei Regolamenti DORA ed eIDAS 2.0, il contributo mostra come le *Distributed Ledger Technologies* possano rafforzare la resilienza digitale e la fiducia computazionale. Ne emerge un possibile nuovo modello di legittimazione digitale del potere pubblico automatizzato.

Parole chiave: RegTech, SupTech, trasparenza, tecnologia dei registri distribuiti (DLT), cibersicurezza.

1. AUTOMATION OF PROCEDURES IN REGTECH AND SUPTECH

It is worth prefacing that the present essay originates from a fruitful transdisciplinary exchange conducted within a research partnership devoted to cryptography and the security of distributed systems. In order to better grasp the potential of such technologies[1] (on which see infra §§ 3 and 7 ff.), we resolved to explore their possible uses and benefits in the field of financial markets, where automation has become a quantitatively significant phenomenon both as a result of policy choices made by individual supervisory authorities and due to the initial innovative impetus autonomously generated by the market itself, which rapidly became a model of efficiency even for public regulators.

Seeking to focus the inquiry on a specific application aligned with our legal expertise, we observed that in recent years supervisory authorities have, with increasing frequency and consistency[2], entrusted technology with functions of regulatory *management*: that is, with the processes of regulatory shaping, which we designate with the term RegTech (regulatory technology), and with technologically enhanced supervisory activities, referred to as SupTech (supervisory technology)[3], meaning the technologically advanced oversight conducted by the public supervisor.

*Il contributo è stato approvato dai revisori.

** *This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU*. Although the paper represents a unified line of inquiry jointly developed by both authors within the project, for attribution purposes it is specified that Sections 1, 4, 4.1, 5, and 6 were written by Michela Passalacqua, while Sections 3, 7, 8, 9, 10, 11, and 12 were authored by Tamara Favaro. Section 2, addressing the research question, was jointly drafted by the authors.

[1] The research unit of the University of Pisa is responsible for the AQuSDIT project (Advanced and Quantum-safe Solutions for Digital Identity and Digital Tracing), within the Extended Partnership "Security and Rights in the Cyberspace", Spoke 5 "Secure and Traceable Identities in Distributed Environments (STRIDE)". The present contribution falls within Sub-task 2: "Digital identification and tracing based on distributed ledger technology".

[2] See European Commission, *Public Sector Tech Watch: Adoption of AI, Blockchain and other emerging technologies within the European public sector*, Publications Office of the European Union, Luxemburg, 2024, pp. 39-40 and 48, which also highlight a comparison between the more widespread use of AI and that of blockchain.

[3] In the legal scholarship, see M. RABITTI, A. SCIARRONE ALIBRANDI, *RegTech e SupTech*, in A. PAJNO, F. DONATI, A. PERRUCCI (ed.), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. III, il Mulino, Bologna, 2022, pp. 451 ff.; I. ANAGNOSTOPOULOS, *Fintech and Regtech: Impact on regulators and banks*, in *Journal of Economics and Business*, n. 100, 2018, pp. 7 ff.

Strictly speaking, RegTech originates in the practice of supervised intermediaries employing technology for self-monitoring compliance with regulatory requirements. Unsurprisingly, the different phenomenon here under examination has begun to be identified in the literature also under the label Reg-RegTech[4], indicating a form of regulation generated by automated control, an approach that, as we shall see, is destined to assume an increasingly prominent and expansive role (*infra* § 4).

Regulators have themselves opted to automate administrative procedures within their remit, seeking gains in efficiency – understood in terms of shorter procedural timeframes – and in effectiveness, measured by the improved quality of outcomes. This objective is pursued by relying, with growing frequency, on digital platforms integrated with artificial intelligence systems for the performance of public functions[5].

In this context, however, the use of AI to support decision-making remains particularly delicate[6], since even a seemingly minimal "algorithmic check" (for specific examples, *infra* § 4) will, in substance, be unlikely to avoid influencing human oversight[7]. One need only consider that, even for systems capable of being classified as high-risk under the European AI Act, it is difficult to determine when the "material" influence of the algorithm on decision-making may be considered absent. Such an assessment cannot be conducted prognostically by the provider or certifier[8]; rather, it can only be cautiously carried out ex post by examining a domain that is intrinsically subjective, namely, the formation of the deployer's will.

[4] On the evolution of the terminology, see L. AMMANNATI, *Regolatori e supervisori nell'era digitale: ripensare la regolazione*, in *Giur. cost.*, n. 3, 2023, pp. 1465 ff. and pp. 1471 ff.

[5] Following the adoption of the European AI Act (Regulation (EU) No. 1689/2024 of the European Parliament and of the Council of 13 June 2024), the Italian implementing legislation aligning the national legal order (Law No. 132 of 23 September 2025, *Provisions and Delegations to the Government on Artificial Intelligence*), in Article 14 on the use of AI by public administrations, codifies efficiency as a goal to be pursued through the reduction of the time required to conclude administrative procedures and the increase in the volume of services provided. The same provision also includes, among its objectives, the pursuit of service quality. As noted by A. MARCHETTI, Report to the Doctoral Seminar *Intelligenza artificiale e diritto*, Pisa, 18 November 2025, these objectives are difficult to reconcile, at least in light of the current state of knowledge.

[6] Article 14 of Law No 132/2025, referred to above, prohibits Italian public administrations from relying on algorithms that entirely replace human decision-making, mandating in all cases their non-exclusivity. Such non-exclusivity is construed in a particularly restrictive manner, namely as mere usability "in a merely *instrumental and supportive* capacity (emphasis added) to administrative decision-making, with due regard for the autonomy and decision-making power of the individual, who remains solely responsible for the adopted measures". The hendiadys "instrumental and supportive" appears to exclude the legitimacy of algorithms that assist the public official to such an extent as to deprive any non-automated component of the decision of independent relevance. Had the legislature confined itself to referring solely to "instrumental algorithms", it would have remained possible to admit decisions entirely dictated by the algorithm, albeit formally subject to a simple human 'sign-off'.

[7] A critical assessment of the excessive reliance on technology by the Italian public administration is offered by G. AVANZINI, *Intelligenza artificiale, machine learning e istruttoria procedimentale: vantaggi limiti ed esigenze di una corretta Data Governance*, in A. PAJNO, F. DONATI, A. PERRUCCI (eds.), *op. cit.*, vol. II, esp. p. 86. Drawing on findings from behavioural science in order to assess the effectiveness of the human-in-the-loop requirement, see human in the loop, A. MARCHETTI, *Intelligenza artificiale, poteri pubblici e rule of law*, in *Riv. it. dir. pubbl. comunit.*, n. 1, 2024, pp. 54-55.

[8] With regard to the conformity assessment of high-risk AI systems – carried out either under the provider's internal control or by notified conformity assessment bodies, which in some cases coincide with the competent market surveillance authorities – see Articles 43-45 of Regulation (EU) 1689/2024, cited above.

Moreover, the use of algorithms in RegTech and SupTech will not, as a rule, trigger the safeguards of the AI Act, which may be invoked only in relation to the automation of sensitive sectors or, in a far more limited respect, for the physical security of the deployed platform[9].

2. THE RESEARCH QUESTION: CAN THE OPACITY OF ALGORITHMIC REGULATION BE REMEDIED BY BLOCKCHAIN TECHNOLOGY?

Having briefly outlined the role that RegTech and SupTech platforms are increasingly assuming (*supra* § 1), it must be noted that they are progressively absorbing functions traditionally exercised by public authorities, through the translation of administrative procedures into computational rules and algorithmic logics underpinning data-driven models[10]. As a result, while recourse to automation through artificial intelligence systems on the one hand lends itself to accelerating and simplifying administrative procedures, on the other hand it gives rise to significant difficulties in ensuring the traditional forms of oversight over administrative action. Such oversight should, in the first instance, be guaranteed by the administration itself, subsequently by the citizen-user, and ultimately by the courts.

Instead, as will be argued below (*infra* § 4), AI used as a regulatory and supervisory technology assumes an autonomous normative role, capable of shaping the conduct of operators and, consequently, market dynamics, without any corresponding mechanism of accountability or, even prior to that, of explainability of the inferences resulting in prescriptions or, at any rate, in guidance[11].

The opacity of these processes emerges in a particularly stark manner in a recent case brought before the highest administrative court[12]. The judicial decision failed to resolve the issues outlined above, limiting itself to affording protection to the AI system provider, which was strongly shielded by the existing regimes of intellectual property protection. These regimes influenced the interpretative outcome leading to the denial of access to the source code requested by the applicant. In brief, the digital platform used by the public administration indicated that a specific document included in a technical offer for the award of a public contract did not correspond to the same document previously marked by the generation of a digital fingerprint within the deadline imposed by the procedure. This was evidently a discrepancy that could not be materially detected, unlike what would have occurred in the case of a physical document deposited in hard copy.

The case law thus demonstrates the urgent need to accompany technological innovation with new forms of protection for non-technical subjects. It is not conceivable to leave the explainability of algorithms exclusively

[9] On this issue, for further analysis, reference may be made to M. PASSALACQUA, *FinTech e regolazione digitale. Verso una cyber-vigilanza?*, in P. GAGGERO (ed.), *Regulating Technological Driven Finance*, Cacucci, Bari, (forthcoming), § 4.

[10] For the distinction between computational rules and algorithmic rules, see *infra* § 4.1.

[11] In this contribution, the notion of algorithmic regulation is used in a broad sense, encompassing both rule-based computational implementations and algorithmic prescriptions, whose analytical distinction will be developed below (*infra* § 4.1).

[12] Italian Council of State (Consiglio di Stato), section IV, judgment of 4 June 2025, no. 4857.

to litigation and technical expert evidence – as indeed occurred in the case at hand – without tolerating an unacceptable regression in the guarantees afforded to citizens *vis-à-vis* the administration. It is worth noting that the algorithm in question was not decision-making (a category unanimously regarded as more pernicious and now prohibited for Italian public administrations[13]), but merely supportive of the decision, confirming that even such technologies are far from innocuous with respect to the resilience of the rule of law.

What thus emerges is a crisis of the legitimacy of power: who controls the algorithm that regulates?

Our thesis is that technology itself may offer the tools to address the problems it generates. The criticalities of procedural automation would be significantly reduced if blockchain technology were capable of certifying the algorithms employed in administrative activities.

Ultimately, our research question is as follows: if regulation has become computational, why should its legitimacy not also be rendered computationally verifiable through blockchain?

In other words, if – as we shall show (*infra* §§ 4 and 4.1) – regulation becomes code, then legitimacy must become algorithm. Distributed Ledger Technology thus comes into play as a potential instrument to restore traceability[14] and verifiability to the circuit of public accountability.

This gives rise to a form of techno-supervision based on blockchain, capable of ensuring transparency, accountability and the trust required for the increasingly widespread use of digital technologies in regulation and supervision.

The phenomenon may also be described as cyber supervision: a model that does not merely concern traditional digital security oversight, where the object of the activity is "cyber", but instead extends to the very architecture of verification, rendering "cyber" the means through which such oversight is exercised.

The underlying idea advanced in this contribution is therefore to employ Distributed Ledger Technologies not only as specific RegTech and SupTech tools, but also as an infrastructure for meta-supervision.

This analysis has been conducted with reference to a specific "normative case", represented by the Digital Operational Resilience Act (DORA) (*infra* §§ 6 ff.), in order to assess, within the banking and financial market context, whether and how distributed ledger technologies may simultaneously ensure not only effective cyber supervision, but also a form of meta-supervision grounded in an infrastructure of trust, capable of restoring transparency and legitimacy to automated regulatory power.

[13] See *supra* note 6.

[14] The aforementioned Article 14 of Law No. 132/2025 requires public authorities to ensure the "traceability" of the algorithms used in administrative activities, without, however, specifying the means by which such a standard is to be achieved, a standard that, depending on the specific use case, may prove to be particularly demanding. By way of example, while it is relatively straightforward to make the deterministic processes of a chatbot expressly traceable through their translation into natural language, it is far more complex to render the functioning of a data acquisition system transparent without disclosing its source code.

3. TOWARDS A DISTRIBUTED MODEL OF META-SUPERVISION

Understanding why Distributed Ledger Technology has acquired such a decisive role in contemporary architectures of control requires returning to the conceptual assumptions that shaped its earliest theoretical formulations. In its initial phase, blockchain technology – and, more broadly, the distributed ledger paradigm as a whole – was presented as a form of self-sufficient private regulation, removed from the oversight and protection of the legal order and entrusted instead to the governance of machines and algorithms[15]. It was, in fact, embedded within the ideological horizon of libertarian crypto-anarchism, from which the so-called *Cyberpunk Manifesto* emerged in 1993[16]. Within this framework, code was endowed with the capacity to replace central authority[17], giving rise to a model of computational trust grounded in the immutability of digital inscriptions and in the mechanism of distributed consensus[18].

Against this backdrop, *Lex Cryptographia* took shape as an alternative normative order, aimed at redefining the organisation of political, economic and social interactions and at calling into question the traditional role of the State and public institutions. Within this vision, code did not merely express the rule, but directly incorporated its enforcement power[19].

As anticipated, however, this "rebellious genealogy" now appears largely as a legacy of the formative phase and no longer corresponds to the dominant perspective through which blockchain technology is studied and deployed today. Contemporary analyses tend instead to situate it within the paradigms of RegTech and SupTech, conceiving it primarily as a technology in support of regulation and supervision[20].

Yet a return to its original ideological matrix allows one to move beyond such a merely instrumental reading. The aspiration towards alternative forms of normativity and the displacement of authority through

[15] For an earlier discussion of this issue, please see T. FAVARO, *Blockchain per l'intervento pubblico. Un possibile ritorno ai "luoghi" dell'economia*, in A. ANTONUCCI, M. DE POLI, A. URBANI (eds.), *I luoghi dell'Economia. Le dimensioni della sovranità*, Torino, Giappichelli, 2019, p. 39.

[16] See C. KIRTCHEV, *A Cyberpunk Manifesto*, available at: *http://project.cyberpunk.ru/idb/cyberpunk_manifesto.html*. For an account of the evolution of blockchain technology and of the intellectual currents that inspired its emergence, see F. SARZANA, M. NICOTRA, *Diritto della Blockchain, Intelligenza Artificiale e IoT*, Ipsoa, Assago, 2018, p. 9 ff. In particular, the Cyberpunk movement seeks to counter the potential erosion of individual freedoms resulting from the growing pervasiveness of information technologies, which enable governments and large corporations to monitor and correlate personal data derived from everyday transactions. In response to this risk, the movement promotes the development of anonymous electronic currency and untraceable payment instruments, grounded in widely distributed cryptographic techniques, which are also capable of enabling secure messaging systems, digital contracts, and electronic identities respectful of individuals' informational autonomy.

[17] See M. ATZORI, *Blockchain Technology and Decentralized Governance: is the State Still Necessary?*, in *Journal of Governance and Regulation*, n. 1, 2017, pp. 45-62.

[18] See K. WERBACH, *The Blockchain and the New Architecture of Trust*, MIT Press, Cambridge, 2018, pp. 101-138; V. GUPTA, *The Promise of Blockchain in a World Without Middlemen*, in *Harvard Business Review*, available at: *www.harvard.edu*, 2017.

[19] See P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law. The Rule of Code*, Harvard University Press, Cambridge, 2018, pp. 35-60.

[20] Along these lines, see, for example, F. BASSAN, M. RABITTI, *From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation*, in *Computer Law & Security Review*, vol. 55, 2024, esp. pp. 1-3; P. CHIRULLI, *FinTech, RegTech and SupTech: Institutional Challenges to the Supervisory Architecture of Financial Markets*, in I. CHIU, G. DEIPENBROCK (eds.), *Routledge Handbook of Financial Technology and Law*, Routledge, London-New York, 2021, pp. 447-464.

distributed mechanisms of trust make it possible to conceive of blockchain not simply as a technical aid to regulatory and supervisory action, but as the potential infrastructure of an additional layer of control, directed at scrutinising the very operation of the apparatus through which public power is exercised[21]. The erosion of transparency accompanying the progressive delegation of regulatory functions to algorithmic systems calls for a form of control that does not stop at procedural outcomes, but penetrates the operational logic of the device that generates them.

It is at this juncture that *distributed meta-supervision* emerges: a higher-order, reflexive level of oversight aimed no longer merely at monitoring the behaviour of regulated entities or the formal correctness of the decisions produced, but at examining the technical architecture, internal evolution, and inferential dynamics of the regulatory algorithm itself.

More precisely, distributed meta-supervision may be defined as a second-order control mechanism implemented through distributed ledger infrastructures. Through this mechanism, the activity of the algorithm is recorded in a decentralised digital archive characterised by immutability, traceability, and computational verifiability. Such activity includes the rules embedded in the system, their subsequent modifications, the decision-making pathways, and the logical transformations that underpin its operation.

In this way, blockchain technology appears capable of extracting the regulatory apparatus from the opacity that typically envelops automated processes, restoring to the public sphere the capacity to observe, understand, and contest – on a technically grounded basis – the very genealogy of algorithmic decisions.

Distributed meta-supervision thus takes shape as a mechanism through which public accountability is embedded within a technical infrastructure that is not only resistant to manipulation, but intrinsically transparent and shared. This infrastructure takes the form of a computational archive in which the transformations of the regulatory algorithm – its implementations, weighting criteria, deductive logics, and successive revisions – are preserved in an indelible manner. It thereby becomes possible to reconstruct, in an objectively verifiable way, the circuit of legitimation that recourse to automation risks dissolving, reaffirming that the exercise of regulatory power must be not only lawful, but also scrutable in its technical substance and therefore open to epistemic and procedural contestation.

Such a configuration does not purport to supplant traditional instruments of control, nor does it aspire to replace human judgment with yet another layer of automation. Rather, it introduces an additional level of guarantee, indispensable in an environment in which regulatory functions are increasingly entrusted to digital entities whose operations elude the classical canons of administrative transparency. Distributed meta-supervision thus represents an attempt to re-found the legitimacy of regulatory power within the computational ecosystem, by providing an infrastructure that enables the stable, independent, and technically

[21] See M. ALLENA, *Blockchain Technology and Regulatory Compliance: Towards a Cooperative Supervisory Model*, in *European Review of Digital Administration & Law*, n. 2, 2021, pp. 37-43, who highlights how blockchain enables forms of distributed compliance verification and polycentric supervision, anticipating models of control that move beyond the traditional dichotomy between supervisory authorities and supervised entities.

controllable observation of the deep functioning of the algorithmic device.

For this very reason, distributed meta-supervision finds its most compelling testing ground in those sectors in which algorithmic regulation is already operational and institutionalised. Financial markets – by virtue of the intensity of supervision, the technical complexity of the instruments involved, and the centrality of digital supervisory infrastructures – constitute the context in which these dynamics emerge with particular clarity and call for focused reflection.

4. ALGORITHMIC REGULATION IN FINANCIAL MARKETS

In the banking and financial sector, a growing number of digital platforms are being deployed by supervisory authorities to monitor, analyse and oversee the activities of market operators. These platforms support core functions, including automated data collection, the formal and substantive validation of regulatory reporting, compliance monitoring, risk and anomaly analysis, information exchange with supervised entities, and interoperability among national and European authorities.

In Italy, two platforms developed by the central bank deserve particular mention: Infostat, used for the submission of statistical and supervisory reports by banks, financial intermediaries and other operators, and Puma2 (Unified Procedure for Corporate Reporting Matrices), designed for the automated production of supervisory reports and the transformation of accounting data into regulatory reporting[22]. Also noteworthy is Sipaf, the Integrated System for Financial Publication and Analysis operated by Consob (Italian Securities and Exchange Commission), which is used to monitor and collect information on listed companies.

At the European level, the IMAS Portal enables the ECB to carry out banking supervision by managing authorisation procedures and information-based supervisory activities. Reference should also be made to the Firds & Fitrs IT systems. The former is a database introduced by the MiFID II Directive[23], while the Financial Instruments Transparency System is the database used by ESMA for the collection and publication of financial data (financial instruments, transparency and trading obligations), with the aim of safeguarding market integrity.

Supervision carried out through these digital data-collection platforms – often referred to as data-driven supervision[24] – reveals, on the one hand, their inherent tendency towards forms of self-regulation aimed at maximising efficiency and, on the other hand, their capacity to “enable” public regulation, transforming it into an instrument for supporting and steering market behaviour rather than merely correcting market failures.

[22] On this point, see M. CASA, M. CARNEVALI, S. GIACINTI, R. SABATINI, *PUMA cooperation between the Bank of Italy and the intermediaries for the production of statistical, supervisory and resolution reporting*, Bank of Italy occasional paper, no. 734, November 2022.

[23] Directive 2014/65/EU; see also Article 4 of Regulation (EU) No. 596/2014 on market abuse and Article 27 of Regulation (EU) No. 600/2014 (MiFIR).

[24] This terminology is used by Consob, *Piano strategico 2022-2024*, cit., p. 1 e pp. 7 ff.; Id., *Piano strategico 2025-2027*, pp. 7 ff. For a useful case-based analysis, see D. BROEDERS, J. PRENIO, *Innovative technology in financial supervision (SupTech): The experience of early users*, Financial Stability Institute/Bank for International Settlements, Insights on policy implementation, vol. IX, July 2018, *www.bis.org*.

As noted above, the supervisory administrative procedure is progressively being condensed, to the point of being largely absorbed into the operating rules of the platform itself, with evident risks in terms of transparency. The transformation of *lex* into *codex* is by no means neutral for the legal system. The digitalisation of public constraints automatically simplifies them and makes them replicable by machines[25]. As a result, changes and evolutions in conduct become, to some extent, mediated by technology, thereby opening up new spaces in which the technical capabilities of the infrastructure itself may generate novel practical solutions.

From the perspective of data scientists – and increasingly also of regulators and legal scholars – it is widely accepted, for example, that equipping these interoperable, data-aggregating platforms with artificial intelligence[26] systems makes it possible to estimate characteristics that are unknown but relevant to anticipate. This applies, inter alia, to the analysis of credit exposures recorded for supervisory capital purposes in order to identify inadequately recognised expected losses[27]; to predictive assessments aimed at justifying early intervention measures to prevent the crisis of an intermediary[28]; or to stochastic data analyses capable of identifying macroeconomic scenarios and forecasting potential shocks[29]. Further examples include the analysis of informational assets derived from complaints submitted by private parties to supervisory authorities[30], as well as the verification of reports on suspicious transactions related to anti-money laundering (AML) or counter-terrorist financing (CTF)[31]. In certain practical applications, predictive capacity merges with ex post control, as in the analysis of trading data on financial instruments[32] in order to detect or anticipate market manipulation[33], or in the development of new early-warning and rating indicators in the design and distribution of financial

[25] According to Rabitti and Sciarrone Alibrandi, Reg-RegTech may be understood as the translation of legal rules expressed in natural language into computer code, enabling the automated "reading" of legal norms, whether to allow their application by their addressees or to verify their application by the authorities responsible for enforcement; see *op. cit.*, pp. 456-458.

[26] More generally, on the structure and characteristics of platforms *tout court*, including with reference to information-collection systems, see A. CANEPA, *I mercanti dell'era digitale. Un contributo allo studio delle piattaforme*, Giappichelli, Torino, 2020, pp. 35 ff.

[27] As implemented by the Central Bank of Brazil through the ADAM platform (*Amostragem Determinada por Aprendizado de Máquina*), for which further details are analysed by A. CANEPA, *Crisi bancarie e intelligenza artificiale tra prevenzione e nuove vulnerabilità*, in L. AMMANNATI, A. CANEPA, G. GRECO, U. MINNECI (eds.), *Mercati finanziari e transizione digitale. Una tassonomia*, Giappichelli, Torino, 2025, p. 177.

[28] On this issue, see D. ROSSANO, *Gestione delle crisi bancarie e innovazione tecnologica*, in P. GAGGERO (ed.), *Regulating Technological Driven Finance*, Cacucci, Bari, (forthcoming); see also G. LOIACONO, E. RULLI, *ResTech: innovative technologies for crisis resolution*, in *Journal of Banking Regulation*, n. 23, 2022, pp. 227 ff.

[29] A. SIMEONE, *Predictive methods in economics: the link between Econophysics and Artificial Intelligence*, in P. SAVONA, R. MASERA (eds.), *Monetary Policy Normalization. One Hundred Years After Keynes' Tract on Monetary Reform*, Springer, Cham, 2023, pp. 107 ff.

[30] Since 2021, the Bank of Italy has carried out this activity through an AI-based system known as EspTech; on this issue, see M. B. ARMIENTO, *Prove di regolazione dell'intelligenza artificiale: il Regolamento della Banca d'Italia sulla gestione degli esposti*, in *Giorn. dir. amm.*, n. 1, 2023, pp. 105 ff.

[31] R. COELHO, M. DE SIMONI, J. PRENIO, *Suptech applications for anti-money laundering*, Uif, Quaderni dell'antiriciclaggio, October 2019 (published on 9 December 2019); Bank of Italy*, Indagine qualitativa sull'adozione di strumenti innovativi per l'adempimento degli obblighi AML/CFT*, 2 September 2025.

[32] Long since fully automated; see the detailed analysis by N. DE LUCA, *Non più grida dai recinti. L'era delle piattaforme di "trading" e "post-trading"*, in *Analisi giur. dell'economia*, n. 1, 2025, pp. 155 ff.

[33] P. DERIU, S. RACIOPPI, provide a detailed account of machine-learning techniques supporting the detection of insider trading cases, in *Come l'IA può supportare la vigilanza della Consob sugli abusi di mercato*, in *Riflessioni in tema di intelligenza artificiale e attività di vigilanza*, Consob FinTech papers, vol. XV, August 2025, pp. 57 ff.

products and instruments, aimed at predicting and/or curbing phenomena such as greenwashing[34].

All of this shows how public constraints generate large volumes of data that lend themselves to reprocessing. In carrying out this process, platforms display a capacity for self-regulation aimed at maximising the overall efficiency of the system; in doing so, artificial intelligence becomes a candidate for use as a regulatory tool, in the sense in which the term RegTech is employed in this contribution.

Such self-regulation is based on a detailed and enhanced analysis – depending on the case – of balance-sheet data or non-financial information, trading and payment data, and macroeconomic data. It is not unconstrained, but rather bound to the purpose of the administrative procedure, and translates into the possibility of preventing and resolving conflicts at an early stage, thereby avoiding interference with the market's allocative function in the optimal distribution of resources among participants. From this perspective, artificial intelligence does not merely perform an instrumental role of technical support, but progressively assumes a regulatory function: through predictive, automated correction and continuous monitoring algorithms, it directly affects market dynamics by shaping the behaviour of operators. This gives rise to a use of AI not only as a means of efficiency enhancement, but as a genuine regulatory instrument capable of complementing – and in some cases substituting – traditional forms of prescriptive intervention.

In short, a normative dimension of artificial intelligence is emerging[35], one that is capable of significantly increasing the efficiency of numerous activities. As previously noted, it may thus be argued that platforms are destined to "enable" regulation: by intervening at a granular level, starting from individual cases[36], they are able to correct inefficiencies. This may lead to new regulatory practices and to a reversal in the sequence of regulation. Given the machine's ability to penetrate the specificity of individual cases through rapid data processing, computational power can then be used to abstract generalisable prescriptive rules. By way of example, it is

[34] Consob has developed two prototypes based on machine-learning and natural language processing techniques, aimed respectively at detecting greenwashing phenomena in the design and distribution of financial products and instruments, and at identifying anomalous behaviours and potential cases of market abuse. The latter, known as Pandora Box, has been developed as a minimum viable product (MVP); source: Consob, *Piano strategico 2025-2027*, cit., p. 8, see also p. 20. Further details are provided by S. PATERLINI, A. NICOLODI, M. GENTILE, V. FOGLIA MANZILLO, M. R. SANCILIO, P. DERIU, *Greenwashing alert system for EU green bonds. The Consob-University of Trento prototype*, Consob FinTech papers, vol. XIV, July 2025. Consob appears to be among the authorities that have launched the largest number of initiatives to experiment with the use of AI in supervisory activities; for an overview, see P. DERIU, S. RACIOPPI, *ibidem*.

[35] This view is also endorsed by M. R. FERRARESE, *Poteri nuovi. Privati, penetranti, opachi*, il Mulino, Bologna, 2022, p. 73, who argues that "platforms and algorithms have a normative substance". Public law scholarship, in acknowledging this phenomenon, observes that the spread of technology and artificial intelligence exposes public administrations to "rules not produced by traditional sources of law", F. FRACCHIA, *Lo spazio della pubblica amministrazione. Vecchi territori e nuove frontiere. Un quadro d'insieme*, in *Dir. dell'economia*, n. 2, 2023, p. 301 citing R. FERRARA, *La globalizzazione e il diritto pubblico*, in *Federalismi*, n. 19, 2023, pp. 23 e ss. More specifically, on the normative use of AI, see the early reflections by L. AMMANNATI, F. DI PORTO, *L'intelligenza artificiale per la fornitura di servizi, di applicazioni e la produzione di regole:* Digital Services Act, Digital Markets Act *e* Artificial Intelligence Act, in A. PAJNO, F. DONATI, A. PERRUCCI (eds.), *op. cit.*, vol. I, pp. 479 ff.; L. AMMANNATI, F. COSTANTINO, *Intelligenza artificiale e regolazione dei mercati digitali. Modelli di regolazione e di regolatori*, *ibid.*, pp. 547 ff.; F. DI PORTO, A. SIGNORELLI, *Regolare attraverso l'intelligenza artificiale*, *ibid.*, pp. 617 ff.

[36] For a more in-depth analysis of this case-law, see in particular T. FAVARO, *Artificial Intelligence in Italian Public Administration. Challenges, case-studies and regulatory perspectives*, in *Journal für Rechtspolitik*, n. 1, 2023, pp. 60-73; M. DUGATO, D. VESE, *Intelligenza artificiale, amministrazione e tutela dei diritti*, in M. PALMIRANI (ed.), *La trasformazione digitale della giustizia nel dialogo tra discipline. Diritto e Intelligenza Artificiale*, Giuffrè, Milano, 2022, pp. 183 ff.

entirely feasible to develop recommendation systems (search engines) that provide guidance on the reliability of economic operators with respect to the environmental sustainability of financial products and instruments.

4.1. TYPES OF DIGITAL RULES: COMPUTATIONAL PROVISIONS AND ALGORITHMIC PRESCRIPTIONS

The recourse to platforms tends to generate digital rules[37]. These rules are inherent in the platform itself and encompass both strictly computational provisions resulting from the automated conversion of legal norms (so-called *computational rules*), and prescriptions governing future conduct deriving from the "predictive pace" of the algorithms in use (so-called *algorithmic rules*), as discussed above (*supra* § 4).

As regards digital rules of the first type, namely computational rules in the strict sense, the banking and financial markets have arguably been among their earliest fields of application. Consider, for example, the automatic blocking mechanisms for transactions exceeding the risk or leverage limits laid down by the MiFID II framework[38], or the algorithmic filters increasingly employed by intermediaries to assess *ex ante* the suitability or appropriateness of an investment in relation to the user's profile, thereby preventing the execution of non-compliant orders[39]. Similar examples may be found in payment systems governed by the PSD2 Directive[40], where platforms automatically reject transactions lacking Strong Customer Authentication or failing to comply with technical access standards[41].

[37] With specific reference to the peculiar software programs known as smart contracts, Nuzzo observes that technology has "its own procedural rules, which reduce personal self-determination and subjective intentions to the binary language inherent in programming"; see A. NUZZO, *Algoritmi e potere*, in *Analisi giur. dell'economia*, n. 1, 2019, p. 42.

[38] Articles 24-25 and 48 of Directive 2014/65/EU, cited above, and Articles 54 ff. of Commission Delegated Regulation (EU) No. 2017/565, concerning risk management and operational limits, as well as Article 12 of the Markets Regulation, adopted by Consob pursuant to Resolution No. 20249 of 28 November 2017, as amended.

[39] On the need to assess "digital suitability" in investment services, see M. MENGONI, *La nuova strategia della Commissione Europea in tema di finanza digitale:* quid iuris *per i (futuri) servizi finanziari offerti dalle società* Tech, *Paper di diritto europeo*, 2021, pp. 122-123; A. DAVOLA, *Gli algoritmi nell'attività finanziaria*, in FinTech*,* financiatization *e rivoluzione digitale: coordinate del fenomeno, ed impatto sugli assetti operativi dei mercati*, in *Algoritmi decisionali e trasparenza bancaria. Il paradigma dell'inerenza nella regolamentazione delle tecnologie emergenti*, Utet, Milano, 2020, pp. 91 ff. See also the ESMA Guidelines of 12 April 2022 *on certain aspects of the MiFID II appropriateness and execution-only requirements* under MiFID II (ESMA 35-43-3006), concerning automated controls, paras 91-93. Reference should further be made to Commission Delegated Regulation (EU) No. 589/2017 on pre-trade controls under the MiFID II framework, which specifies the organisational requirements for investment firms engaging in algorithmic trading.

[39] Articles 97 and 98 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 address strong customer authentication and access to payment accounts through standardised interfaces.

[40] Articles 97 and 98 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 address strong customer authentication and access to payment accounts through standardised interfaces.

[41] *Application Programming Interface* (*API*), namely application programming interfaces; see Commission Delegated Regulation (EU) No. 2018/389 of 27 November 2017, supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards on strong customer authentication and common and secure open standards of communication, adopted on the basis of the final report of the European Banking Authority (EBA), *Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication* (EBA/RTS/2017/02, also known as the "*EBA RTS on SCA & CSC*"). See also EBA, *Opinion on the Implementation of the RTS on SCA and CSC*, 21 June 2019.

In all these cases, the legal rule – aimed at ensuring the fairness, security or transparency of financial activity – is translated, either by operation of law or through self-regulation by the parties, into a technical constraint embedded in the platform's code[42]. It thus assumes the nature of a digital rule "implanted" in the platform's operational architecture and co-essential to the functioning of the automated system itself.

Such technical rules do not merely support the technology in use, but directly implement the legal norm[43], binding operators *ex ante* and eliminating any margin of applicative discretion; they are, in other words, *hard coded*.

Algorithmic rules[44], by contrast, arise from the operation of platforms through the deployment of "AI-based methodologies"[45] and, as noted above, display the capacity to orient future conduct.

It is therefore unsurprising that attentive scholarship had already observed that, in FinTech sectors most deeply shaped by algorithms – such as high-frequency trading, robo-advisory services and creditworthiness assessment – artificial intelligence shifts "from being a productive factor of the organisation to becoming the organisation of productive factors itself"[46], thereby assuming an autonomous, non-instrumental role.

These rules, which we term algorithmic because they derive directly from the functioning of the machine[47], possess significant potential to accelerate the processes to which they apply, while at the same time giving rise to new risks[48].

For present purposes, a first conclusion may be drawn. The normative vocation of automated systems requires the application of rules governing the functioning of the digital market that serve as a guarantee of a precondition for competition, always with a view to maximising efficiency. What thus emerges is a regulatory

[42] On the notion of "digital rules" as the technical embodiment of normative prescriptions, see L. FLORIDI, *The Logic of Information*, Oxford University Press, Oxford, 2019, pp. 201 ff.; L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

[43] It is, of course, necessary to pay close attention to the specific features of the enabling technologies to which reference is made. With regard to Distributed Ledger Technologies (DLT), or blockchain, for example, a distinct assessment is required, insofar as computer code itself comes to operate automatically as a legal rule. On this issue, see A. ANTONUCCI, *La controvertibile fiducia verso la matematica: il codice informatico come regolatore*, in *I non-luoghi di produzione delle regole*, in A. ANTONUCCI, M. DE POLI, A. URBANI (eds.), *I luoghi dell'economia. Le dimensioni della sovranità*, Giappichelli, Torino, 2019, pp. 20 ff., who illustrates, with reference to bitcoin, the displacement of the "natural" legislator, since regulation is entrusted to autonomous "processes and mechanisms defined by the computational architecture". In a similar vein, see P. DE FILIPPI, S. HASSAN, *Blockchain technology as a regulatory technology. From code is law to law is code*, in *First Monday*, 2016, p. 12.

[44] The proposed terminology appears to be confirmed by a similar usage in K. YEUNG, *Algorithmic Regulation: A Critical Interrogation*, in *Regulation & Governance*, n. 4, 2017, pp. 505 ff., and further developed in several of the contributions collected in K. YEUNG, M. LODGE, (eds.), *Algorithmic Regulation*, Oxford University Press, Oxford, 2019.

[45] The effective expression is due to B. GALGANI, *Ragioni e conferme di una "visione"*, in *Processi, rappresentazioni e piattaforme digitali* (ed.), Giappichelli, Torino, 2023, XIII.

[46] P. LUCANTONI, *L'high frequency trading nel prisma della vigilanza algoritmica*, in *Analisi giur. dell'economia*, n. 1, 2019, p. 297, as cited by R. LENER, *Il paradigma dei settori regolati e la democrazia dell'algoritmo. Note introduttive*, in *Riv. dir. bancario*, supplement 2020-2021, pp. 198-199.

[47] For an illustrative example, see *supra* § 4.

[48] First, negative externalities, potentially capable of generating systemic risks, arising from biases or errors in the construction of datasets or in the functioning of algorithms; see C. O'NEIL, *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*, Crown Pub, New York, 2016, (Italian trans., *Armi di distruzione matematica*, Bompiani, Firenze, 2017); S. BAROCAS, A. D. SELBST, *Big Data's Disparate Impact*, in *California Law Review*, n. 3, 2016, pp. 671 ff. In legal scholarship, see the comprehensive overview by A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giur. dell'economia*, n. 1, 2019, pp. 47 e ff.

and managerial power exercised by platforms that does not presuppose a market failure, but rather a form of market discipline, partly constituted by digital rules.

The distinction outlined between computational provisions and algorithmic prescriptions should not, however, be understood as rigid or impermeable. Transfers between the two categories are in fact possible: there are instances in which a computational rule evolves into an algorithmic rule of governance (cf. *infra* § 9); conversely, a check performed through an "algorithmic filter" may amount to a purely computational rule, for example by generating an automatic suspension of activity.

5. DATA SHARING AND COMPUTATIONAL TRUST

RegTech and SupTech operate most effectively in ensuring efficient supervision when two preliminary conditions are met: interoperability and data governance. Within the domestic legal framework, interoperability makes it possible to leverage the services of the National Data Platform (Piattaforma Digitale Nazionale Dati – PDND)[49], thereby enabling data sharing, which in turn presupposes robust data governance grounded in computational trust.

Not only in the private sector, but also in the public sphere, data thus become assets subject to exchange and valorisation[50], acquiring relevance insofar as they generate positions of dominance. Suffice it to note that, in business law, data sets may be protected by intellectual property rights without temporal limits[51], whereas in the

[49] Managed by the Presidency of the Council of Ministers, it is a technological infrastructure envisaged as early as 2017 and implemented only in 2022 thanks to funding under the National Recovery and Resilience Plan (PNRR). Adherence to it is mandatory for public administrations, providers of public services and non-listed companies controlled by public owners. The infrastructure enables interoperability among information systems and databases, allowing the exchange of information between participating entities in order to enhance the knowledge and use of informational assets held for institutional purposes (see Article 50-ter of Legislative Decree No. 82/2005, as introduced by Article 45(2) of Legislative Decree No. 217/2017). In the legal scholarship, see A. SANDULLI, *Lo "Stato digitale". Pubblico e privato nelle infrastrutture strategiche*, in *Riv. trim. dir. pubbl.*, n. 2, 2021, pp. 513 ss.

[50] As G. FINOCCHIARO aptly observes, "information has been 'entity-fied' and 'reified', becoming 'things'. Data, both personal and non-personal, have become objects of communication and also of valorisation"; see ID., *La sovranità digitale*, in *Dir. pubbl.*, n. 3, 2022, p. 817.

[51] See K. PISTOR, *The Code of Capital. How the Law Creates Wealth and Inequality*, Princeton University Press, Princeton, 2019 (Italian trans., *Il codice del capitale. Come il diritto crea ricchezza e disuguaglianza*, Roma, 2021), who recalls that similar protectionist mechanisms – described as feudal in nature insofar as they evoke the inalienability constraints (*entails*) of medieval guilds – underpin the economic success of major corporations such as Google, Facebook and Amazon. On the protection of datasets as original databases, V. FALCE, *Le regole sulle banche dati nella strategia europea: (molti) diritti e (poche) responsabilità*, in A. PAJNO, F. DONATI, A. PERRUCCI (eds.), *op. cit.*, vol. II, pp. 360 ff.

public sector one often encounters "competitive" assessments among administrations[52], which make them reluctant to pool[53] their informational assets.

Moreover, there are regulatory obstacles to information sharing, primarily linked to the nature of the data that may or may not be shared. At present, public data governance is neither fully transparent nor uniform. In response to such tendencies towards "closure", legal systems promote institutional interoperability, which presupposes the technical interconnection inherent in the functioning of information systems[54].

Within the Italian legal order, the National Data Platform (PDND), acting as a single aggregating entity, enables interoperability among information systems and cloud-based databases, allowing – subject to authentication – the exchange of information among participating bodies, with a view to enhancing knowledge and use of the informational assets held for institutional purposes. Independent administrative authorities entrusted with guarantee, supervisory and regulatory functions are likewise required to accredit with the PDND, develop the relevant interfaces and make their databases available. No special exemption is provided for supervisory systems in the banking and financial sector, which are therefore subject to the same obligation of data sharing among public authorities[55].

At the European level, the Commission is actively promoting the development of data spaces and platforms for data sharing[56]. These initiatives aim to create secure and interoperable digital ecosystems in

[52] This point is also emphasised by A. SANDULLI, *Lo "Stato digitale"*, cit., pp. 513 ff., who outlines the framework of behavioural and regulatory incentives and disincentives. In any event, "failure to comply with the obligation to make one's databases, or aggregated and anonymised data, available and accessible constitutes the failure to achieve a specific result and a significant objective on the part of the managers responsible for the relevant organisational units, and entails a reduction of no less than 30 per cent of the performance-related remuneration and of the additional compensation linked to individual managerial performance, as well as a prohibition on awarding bonuses or incentives within the same organisational units" (Article 50-ter(5) of the Digital Administration Code – *Codice dell'amministrazione digitale*, CAD).

[53] Pursuant to Articles 2(2) and 50-ter of the Digital Administration Code (CAD), for present purposes only the exercise of activities and functions relating to public order and public security, defence and national security, judicial police and economic and financial police functions remain excluded.

[54] This point is clearly explained in Recital 10 of Directive 2009/24/EC, which states that: "The function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function. The parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as 'interfaces'. This functional interconnection and interaction is generally known as 'interoperability'; such interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged."

[55] A. SIMONATI, *I dati detenuti dall'amministrazione, come bene a destinazione pubblica*, in AA. VV., *I beni pubblici. Tradizione e innovazione*, *Annuario 2024*, Editoriale scientifica, Napoli, 2025, pp. 349-350, observes that, whenever the public interest is involved, private parties lose a veto right over undesired data processing and may rely only on data traceability. As the author notes, "indeed, when a subject – let us assume, even voluntarily – provides the public administration with data concerning him or her, it will not always be possible, even where adequate information has been provided, to understand with which other data such information will be correlated. (…) These risks are particularly evident with regard to processing carried out by administrative authorities, given the tendency towards an informal osmosis among public-sector databases, often in the absence of rigorous formal safeguards".

[56] This process culminated in the Data Governance Act (Regulation (EU) No 868/2022 of the European Parliament and of the Council of 30 May 2022 on European data governance, notably Chapter II on the re-use of certain categories of data held by public sector bodies and Chapter IV on data altruism) and in the so-called Data Act (Regulation (EU) No 2854/2023 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data). Particular attention should be paid to Chapter V of the latter, which authorises public bodies

strategic sectors, facilitating the exchange of information among different public and private actors. Interoperability among the systems of the Member States[57] must also be achieved in the banking and financial domain[58]. An initial implementation is entrusted to the ESAP legislative package (European Single Access Point)[59], a centralised system hosted by the European Securities and Markets Authority (ESMA), which will receive financial and non-financial information on companies and their financial products from national collection bodies across the EU, thereby increasing their visibility and expanding the pool of potential investors. Once such a European database is established, it may evidently also be used for data-driven supervision, or SupTech, thus generating forms of algorithmic regulation (*supra* §§ 4 and 4.1).

Ultimately, automated supervision can be effective only if interoperable infrastructures are put in place. However, such infrastructures do not, in themselves, ensure either transparency or accountability of the algorithms operating within them. From this perspective, blockchain technology – when integrated into specific regulatory frameworks (namely eIDAS II and DORA, discussed *infra* §§ 7-9) – may constitute a layer of meta-supervision capable of ensuring computational trust and institutional legitimacy in the algorithmic regulation of markets.

6. TESTING DIGITAL RESILIENCE FOR DATA-DRIVEN CYBER SUPERVISION

The analysis of the most recent innovations applied to the functioning of financial markets highlights the infrastructural dimension of market digitalisation, revealing a regulatory horizon that extends beyond the traditional scope of FinTech, which is generally structured around the services offered[60] and thus characterised by a fragmented legislative approach.

to share data among themselves, with the European Commission, the European Central Bank or other Union bodies in order to address exceptional needs or to comply with obligations laid down by national or EU law, as well as to Chapter VIII, which is devoted to interoperability. In the legal scholarship, see M. R. FERRARESE, *La sovranità è un bene contendibile? Sfide e potenzialità dei poteri globali*, in *Costituzionaismo.it*, n. 2, 2024, p. 123, citing G. RESTA, *La dimensione collettiva dei dati personali*, in *Parole chiave*, n. 9, 2023, p. 103, who notes that "the distinctiveness of the European regulatory approach emerges particularly in the recent Data Governance Act, which entered into force in 2023 and reveals a new, not merely defensive, attitude towards large web-based companies, while also introducing the innovative initiative of 'data altruism', pursuing 'an objective of opening informational silos and harnessing the value of personal and non-personal data present in Europe through the establishment of common data spaces subject to free intra-EU circulation'".

[57] On the issue of information exchange at the European level and the development of interoperable networks, see S. FARO, *Informazione (Società della)*, in M. P. CHITI, G. GRECO (eds.), *Trattato di diritto amministrativo europeo*, special part, vol. III, Giuffrè, Milano, 2007, 2nd edn, pp. 1287 e ff. More recently, see M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e* big data, Editoriale scientifica, Napoli, 2023, which provides a valuable basis for further analysis of the links between information-based supervision and new forms of algorithmic knowledge.

[58] Rabitti and Sciarrone Alibrandi recall the rules aimed at promoting the sharing of financial data within a dedicated "common data space", as already envisaged in the European Strategy for Data; see M. RABITTI, A. SCIARRONE ALIBRANDI, above, p. 452.

[59] It will become fully operational through a three-phase implementation process by 2030.

[60] Ciocca highlights the opportunistic strategy adopted by Big Tech firms in selecting their initial "playing field" among financial activities in which technology is predominant and the (perceived) reputational risk is lower, such as payment systems; see ID., *Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma*, speech delivered at the meeting of the ABI Executive Committee, 18 November 2020, pp. 3-4.

The strongest harmonising vector appears to be the Digital Operational Resilience Act (the DORA Regulation)[61], which lays down obligations concerning the security of networks and systems supporting the business processes of undertakings in the banking and financial sector[62]. Its purpose is to integrate ICT risks into the operational risks borne by financial intermediaries, so that such risks are taken into account in determining the capital requirements designed to ensure their stability. Accordingly, unlike the CER Directive[63], the DORA Regulation is far more focused on cybersecurity aspects[64].

The virtual infrastructures used in financial markets are in fact exposed to significant cybersecurity vulnerabilities and are therefore subject to the NIS2 Directive updating the Network and Information Security framework[65]. The DORA Regulation may be regarded as a specialised articulation of the NIS2 regime[66], while nevertheless resulting in a fully integrated system in which, for certain identified areas, special regulation prevails, whereas the broader NIS2 framework re-expands whenever required by the State's essential functions relating to public security, defence and national security[67].

[61] Regulation (EU) No. 2554/2022 of 14 December 2022; as regards its domestic implementation, see also Legislative Decree No. 23 of 10 March 2025, *Provisions for the Adaptation of National Legislation to Regulation (EU) 2022/2554***.**

[62] For an in-depth analysis, see M. PIGNATTI, *La* cybersecurity *nella digitalizzazione del settore finanziario*, in *Teoria e critica della regolazione sociale*, n. 2, 2024, pp. 157 ff., also with regard to the relationship between NIS2 and DORA; see also, G. SCHNEIDER, *La resilienza operativa digitale come materia di corporate governance: prime riflessioni a partire dal DORA*, in *Riv. corporate governance*, n. 4, 2022, pp. 553 ff.; G. ALFANO, *Rischi informatici nel settore finanziario: strumenti di prevenzione e resilienza operativa digitale*, in *Riv. dir. bancario*, supplement n. 4, 2024, pp. 357 ff.

[63] *Critical Entities Resilience*, Council Directive 2008/114/EC, repealed and replaced by Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022.

[64] Not by chance, with reference to the legislative proposal, P. CIOCCA, *op. cit.*, pp. 5-6, observed that "in the negotiation of the regulation, an issue that will certainly require further scrutiny is the one lying at the intersection between the EU competences of supervisory authorities (both national and European) and matters of national security, which at present remain exclusively within the competence of the Member States. This is a field that has yet to be fully explored".

[65] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (implemented in Italy by Legislative Decree No. 138/2024), which amends Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and repeals Directive (EU) 2016/1148 (the so-called NIS Directive), significantly expands both the personal and material scope of application of the rules on the security of network and information systems and is accompanied by the imposition of detailed requirements. Cybersecurity is in fact governed by an extensive and specialised regulatory framework, within which particular mention should be made of the Cybersecurity Act, namely Regulation (EU) No. 881/2019 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. At national level, this framework has been complemented by Decree-Law No. 105/2019 on cybersecurity, which defines the national cybersecurity perimeter and refers to a number of implementing measures. Finally, mention should be made of the Cyber Resilience Act (CRA), Regulation (EU) No. 2847/2024 of the European Parliament and of the Council of 23 October 2024. In the legal scholarship, see G. ROMAGNOLI, *Lo Stato regolatore e i suoi limiti a fronte del* cyber risk, in *Dir. mercato assicur. e finanz.*, n. 1, 2024, pp. 159 ff.; T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quad. cost.*, n. 2, 2024, pp. 277 ff.; P. GAGGERO, *L'azione normativa del Governo in materia di* cybersecurity, in B. BAILO, M. FRANCAVIGLIA (eds.), *Bilanci e prospettive intorno ai poteri normativi del Governo*, Jovene, Napoli, 2023, pp. 347 ff.; L. PREVITI, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Giorn. dir. amm.*, n. 1, 2025, pp. 60 ff.

[66] In its Recital 16, the DORA Regulation qualifies itself as *lex specialis* with respect to the NIS2 Directive while "at the same time, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555 to ensure consistency with the cyber security strategies adopted by Member States and to allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by that Directive".

[67] On this issue, see R. URSI (ed.), *La sicurezza nel Cyberspazio*, Franco Angeli, Milano, 2023 and in particular ID., *La sicurezza cibernetica come funzione pubblica*, *ibid.*, pp. 7 ff.; MATASSA, *La regolazione della cybersecurity in Italia*, *ibid.*, pp. 21 ff.; L. SCOGNAMILLO, *Cybersicurezza e sicurezza nazionale*, *ibid.*, pp. 71 ff.; L. CALANDRIELLO, *Il perimetro di sicurezza*

The interaction between these different regulatory layers has been effectively captured in the literature by distinguishing between, on the one hand, the "defence of the technological 'fortress', which protects certain interests against attacks aimed at undermining their stability", and, on the other hand, "preventive activity, which materialises in the promotion of infrastructure resilience against potential or actual threats to their functioning, with a view to preventing or mitigating harm to individuals, undertakings operating in sectors crucial to economic life, or democratic institutions"[68]. At these two levels, national security interests[69] and European objectives relating to the protection of the internal market intersect and overlap.

One immediate consequence is the need to harmonise cyber supervision, which becomes a unifying factor for FinTech and is capable of attracting third-party providers of ICT services deemed critical for the financial sector, even when established in third countries, under a specific supervisory regime[70].

Moreover, the increasing reliance on platforms and artificial intelligence systems for the supervision and regulation of financial markets – discussed at length above (*supra* § 4) – would *de iure condendo* require the extension of digital resilience testing also to the public authorities involved. The question then arises as to which body should be entrusted with this specific form of cyber supervision[71]. It would clearly be inappropriate to replicate the system designed for economic operators, as this would amount to inadequate self-monitoring. Nor does it seem feasible to rely on the National Cybersecurity Agency, which at present does not appear to be equipped with the personnel and resources necessary to assume an additional function that would, moreover, often involve complex second-level oversight of highly technical authorities. In any event, this type of regulation – focused on a relatively narrow set of technical instruments of banking supervision – does not seem to raise "sovereignty reservations" comparable to those that have led to the exclusion of central banks from the framework governing critical infrastructures and cybersecurity. It would in any case be possible to exclude activities relating to monetary policy, while subjecting banking supervision to such a regime. From this perspective as well, in providing dynamic security for the functioning of financial market infrastructures, the "neutral" certification offered by blockchain technology, already mentioned above (*supra* § 2), would present significant advantages

nazionale cibernetica, *ibid.*, pp. 139 ff. According to R. URSI, *ibid.*, p. 9, "the objective is not only the self-preservation of the State and its components, but above all the security of individuals, groups, and *economic* and social *entities*, within a neo-Hobbesian framework" (emphasis added)."

[68] R. URSI, *ibid.*, p. 14.

[69] To grasp its complexity and "elusiveness", it suffices to recall that "at the current state of the art, it is possible to derive from the existing legal framework a definition of 'cybersecurity', but not of 'national security'", as noted by M. MATASSA, *Sicurezza cibernetica e nazionale nell'ordinamento multilivello: quale possibile convivenza?*, in *Teoria e critica regolazione sociale*, n. 1, 2025, p. 77.

[70] Recitals 79-83, in particular Recital 81, as well as Articles 2(1)(u), 3(1)(23)-(24), and 31 ff. of the DORA Regulation.

[71] Such cyber supervision would, in general terms, be added to the obligations imposed by NIS2, pursuant to the combined application of Article 6 and Annexes I and III of Legislative Decree No. 138/2024, cited above. It should be recalled, however, that the Bank of Italy is exempt from such requirements, since neither the CER Directive (Article 2(10)) nor the NIS2 Directive (Article 6(35)) includes the judiciary, parliaments or central banks within the scope of public administration (see Article 4(2) of Legislative Decree No. 138/2024). On the evolution that led to the extension of NIS2 to the entire public administration, subject to the aforementioned exclusions on grounds of sovereignty and national security, see M. MATASSA, *La regolazione della* cybersecurity, cit., p. 30.

(*infra* §§ 7 ff.).

Overall, the legislative framework shows that network security is becoming a vector of harmonisation in techno-finance, capable of constructing a unified regulatory framework. It therefore becomes necessary to assess whether the cyber dimension of supervision affects not only the substantive content of control, but also the very means through which such control is structured.

On closer inspection, cyber supervision of intermediaries already appears not as a merely contextual discipline[72], but as a genuine evolution of financial regulation taking on a new configuration[73]. A symbiosis between technology and law emerges, at times almost inextricable. The preventive public intervention envisaged by DORA pursues objectives that, although mediated by the specificities of cybersecurity, largely coincide with the aims of traditional sectoral supervision: the sound and prudent management of supervised entities, overall stability, efficiency and competitiveness of the financial system, transparency and fairness in relations with customers, complemented by the safeguarding of trust in the financial system and the protection of investors.

The evolution of markets thus suggests the need to rethink the traditional structure of financial supervision, creating new space for its expression in cyber terms. New forms of supervision and regulation are emerging as direct products of technological innovation, capable of enhancing both the scope and the effectiveness of public intervention.

7. BLOCKCHAIN AS AN ENABLING INFRASTRUCTURE FOR THE DORA REGULATION

The cyber-oriented transformation of financial supervision requires reflection not only on the expansion of the substantive scope of public oversight, but also on the reconfiguration of the instruments through which it is exercised. Once conceptualised as a structural parameter, digital operational resilience cannot be reduced to organisational arrangements alone; it must be embedded within the technical architectures that sustain the functioning of financial markets. From this standpoint, digital resilience law transcends the mere prescription of conduct, intervening instead in the configuration of the very systems through which regulatory control is operationalised. It is within this framework that the analysis of the DORA Regulation is situated, together with the potential role of blockchain technology, more broadly understood as distributed ledger technologies, as an enabling infrastructure for a form of digital operational resilience conceived *by design*.

Consistently with this approach, the DORA Regulation does not limit itself to requiring the adoption of

[72] In order to better reflect on the "density" of the ongoing transformation, it is worth recalling that the relatively late emergence of a body of cybersecurity law – dating back only to the last decade – is attributable to the relationship between sovereignty and cyberspace, which was initially "conceived as a virtual space detached from the economic and geopolitical problems of the real world"; see M. MATASSA, *La regolazione della* cybersecurity, cit., p. 23.

[73] According to F. SARTORI, *Gestione dei rischi Ict e governance bancaria*, in *Riv. reg. mercati*, n. 2, 2025, the regulatory framework governing ICT risk constitutes "one of the new frontiers of sound and prudent management, not only because it profoundly affects traditional risk safeguards, but also because it defines the very conditions for an intermediary's admission to, and continued presence in, the regulated financial market".

internal procedures; instead, it demands that digital processes be structured in such a way as to render critical events immediately detectable, reconstructable, and verifiable. To this end, it mandates the implementation of ICT incident management systems and of complete and tamper-resistant traceability records covering the entire lifecycle of digital processes (Articles 15-17)[74], as well as, pursuant to Article 28, the assurance of traceability and integrity in relations with third-party providers classified as "critical"[75]. These requirements articulate a conception of resilience grounded in the integration of organisational safeguards and technical architectures.

The same logic informs the sanctioning and corrective regime set out in Title VI of the DORA Regulation, the application of which presupposes the existence of an unbroken chain of custody of ICT incidents and the integrity of the corresponding digital evidence[76]. In light of these provisions, the documentation and traceability of cyber events become the very foundation of legal responsibility and regulatory compliance. Compliance is no longer demonstrated *ex post* through declarations or episodic verifications, but through the structure of ICT systems themselves. It follows that the Regulation requires banks and financial operators to demonstrate that their systems are free from single points of vulnerability, ensure the integrity, availability, and traceability of data and operations, and provide complete and verifiable records throughout the entire operational cycle.

In this context, the need for reliable and non-manipulable digital evidence also acquires particular relevance in relation to the progressive emergence of data-driven models of supervision. The possibility of

[74] In particular, Article 15(c) requires the development of mechanisms capable of enabling the timely identification of anomalous activities and of the criteria triggering the processes for detecting ICT-related incidents; Article 15(a) of the same Regulation further requires that security tools and policies ensure the availability, authenticity, integrity, and confidentiality of data, thereby presupposing the possibility of verifying their reliability and non-alteration. Article 17(2) and (3)(b) additionally mandates the recording of all ICT-related incidents and the adoption of procedures to identify, track, record, categorise, and classify them according to their severity and impact on the affected services, thus enabling the reconstruction of the event and of its underlying causes. Taken together, these provisions delineate a model of operational resilience that does not exhaust itself in organisational safeguards, but requires a technical structuring of digital processes capable of rendering incidents knowable, verifiable, and assessable *ex post* by the supervisory authority.

[75] Indeed, with regard to third-party ICT service providers classified as "critical", Article 28 of the DORA Regulation requires financial entities to establish and maintain a register of information relating to all contractual arrangements with such providers (para. 1). This register must include, inter alia, information on the nature of the services provided, their criticality or materiality, the location of the supported functions, and the main operational dependencies. The same provision further requires that contractual relationships be structured so as to ensure the traceability, accessibility, and integrity of relevant information, as well as the right of competent authorities to access the data necessary for the exercise of their supervisory functions (paras. 2 and 7). These requirements are intended to render dependencies on critical ICT providers knowable and verifiable over time, thereby enabling the *ex post* reconstruction of responsibility and of the risk profiles associated with the outsourcing of essential or important functions.

[76] See Title VI of Regulation (EU) 2022/2554, in particular Articles 50-52, which confer upon the competent authorities powers of investigation, access to information, and the adoption of corrective and sanctioning measures. More specifically, Article 50 grants competent authorities the power to impose corrective measures and administrative sanctions in the event of breaches of the obligations laid down by the Regulation, while Articles 51 and 52 govern the exercise of supervisory and investigative powers, including the ability to request information, access documentation, and carry out inspections.

The effective exercise of these powers is contingent upon the availability of reliable documentation of ICT-related incidents, consistent with the obligations of recording, traceability, and retention of information set out in Articles 15-17. It follows that the effectiveness of the sanctioning framework presupposes the integrity and continuity of the digital evidence relating to the critical event, thereby configuring a genuine informational chain of the incident that is relevant for the purposes of legal responsibility.

exercising continuous and proportionate oversight over digital operational risks presupposes the availability of structured information flows capable of being processed through automated tools without undermining the attribution of supervisory decisions to public authority. It is from this standpoint that blockchain technology may be understood as a potential enabling infrastructure, not as an instrument for automating supervision, but as a mechanism for guaranteeing the integrity, traceability, and verifiability of the data that underpin supervisory activity[77]. In this sense, blockchain contributes to strengthening the epistemic foundations of data-driven supervision, insofar as it stabilises and renders reliable the data upon which supervisory analysis is based, thereby reducing information asymmetries between intermediaries and supervisory authorities.

Although the Regulation never explicitly refers to systemic risk, its ultimate orientation is clearly towards its prevention[78]. This emerges, first and foremost, from the attention devoted to critical ICT third-party providers and to mechanisms of operational continuity, since an entity is deemed operationally resilient only insofar as it is capable of ensuring the continuity of its critical functions even in the presence of ICT incidents or external disruptions. The objective is thus to prevent dependence on a single infrastructure or provider from generating a concentration of risk capable of undermining the overall stability of the European financial system. From this perspective, operational continuity is not conceived as a mere managerial obligation, but as a constitutive requirement of digital resilience.

Within this framework, the dialogue between the categories of economic law and the language of computer science reveals a significant conceptual convergence. The legal notion of risk concentration proves functionally analogous to the technical concept of a Single Point of Failure (SPOF)[79]. Both describe a condition of systemic vulnerability in which reliance on a single infrastructure or control node exposes the entire system to the risk of disruption or collapse[80]. Such functional concentration therefore runs counter to the principle of operational continuity, since the failure or attack of the critical node would result in a comprehensive interruption

[77] In this regard, see S. GRIMA, M. KIZILKAYA, K. SOOD, M. ERDEMDELICE, *The Perceived Effectiveness of Blockchain for Digital Operational Risk Resilience in the European Union Insurance Market Sector*, in *Journal of Risk and Financial Management*, n. 8, 2021, p. 363. On the basis of an empirical investigation, the authors show that financial market participants perceive blockchain as a tool capable of strengthening certain aspects of digital operational resilience as outlined by the DORA Regulation, owing to its reliability, flexibility, and relevance in the management of operational risk. The study, however, remains confined to the level of market perceptions and does not undertake a legal or techno-architectural assessment of compliance with regulatory requirements.

[78] See L. JANČIŪTĖ, *Cybersecurity in the Financial Sector and the Quantum-Safe Cryptography Transition: In Search of a Precautionary Approach in the EU Digital Operational Resilience Act Framework*, in *International Cybersecurity Law Review*, n. 6, 2025, pp. 145-154, who highlights how, in the financial sector, cyber threats may transcend the dimension of operational risk and come to constitute systemic risks, due to the deep digital interdependence that characterises financial infrastructures. In particular, the author emphasises that a severe ICT incident may rapidly propagate throughout the financial system, undermining essential functions and operators' trust, with potentially macroeconomic effects.

[79] In computer science, a Single Point of Failure is defined as any component of a system that concentrates an essential function in the absence of alternatives or redundancies, such that its malfunction, compromise, or unavailability is capable of causing the disruption or serious impairment of the system's overall functioning.

[80] In partially convergent terms, albeit on a political and organisational plane, see M. ATZORI, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, above, where state centralisation is described as a Single Point of Failure. The author employs this category to criticise the concentration of public power; in the present contribution, by contrast, the notion is used as a functional interpretative key for the prevention of systemic risk, with a view to ensuring digital operational resilience.

of the service.

When read in this light, the requirements imposed by the European Regulation on digital operational resilience, namely integrity, availability, traceability, and verifiability of information, correspond to the properties structurally ensured by decentralised architectures. Without explicitly referring to them, the regulatory framework established by DORA appears oriented towards technological models capable of guaranteeing the non-repudiation of digital records and the stability of evidentiary data throughout the entire lifecycle of ICT processes. In other words, the Regulation does not merely aim to enhance the security of financial markets, but contributes to shifting the centre of gravity of regulation from the behaviour of operators to the configuration of infrastructures. In this sense, distributed ledger technology may be read as an infrastructure particularly consistent with regulatory requirements of immutability and retrospective verifiability of data, reducing the risk of alteration or manipulation of information relating to ICT incidents and relations with third-party providers.

A DLT-based system is capable of strengthening the mechanisms of due diligence and continuous monitoring required by the Regulation by offering a distributed and tamper-resistant record of providers' security posture and of critical interactions. In this way, the principles of operational resilience *by design* enshrined in the DORA Regulation, and in particular the requirement to avoid single points of vulnerability (Non-SPOF), find a possible architectural translation capable of rendering computationally operational the normative resilience imposed by European law.

8. THE EIDAS 2.0 REGULATION AND DIGITAL IDENTITY SYSTEM RESILIENCE

In the same vein, the technical resilience outlined by the Digital Operational Resilience Regulation can be fully achieved only if it rests upon a legally recognised trust infrastructure. In the absence of reliable mechanisms of identification and authentication, the traceability of events, the non-repudiation of operations, and the attribution of responsibility would be structurally compromised. From this perspective, Regulation (EU) 2024/1183 (the so-called eIDAS 2.0 Regulation) constitutes a necessary complement to DORA, as it ensures the uniform legal validity of digital identities, signatures, and attestations across the Union for the purposes of subjective attribution, evidentiary effectiveness, and the non-repudiation of digital operations. Although apparently distinct, the two regulatory instruments are in fact complementary pillars of the Digital Finance Package, united by the common objective of constructing a European infrastructure of trust and operational reliability for the digital economy.

Accordingly, Article 5-septies of Regulation (EU) 2024/1183 requires Member States to ensure that certain entities, including those operating in the financial sector, accept European Digital Identity Wallets (EUDI

Wallets)[81] for electronic authentication and access to services whenever strong authentication is required[82]. Since operational resilience presupposes the reliable identification of users and the secure management of access rights to systems supporting essential or important functions, the EUDI Wallet may be functionally qualified as a mechanism of Strong Customer Authentication[83] for access to regulated digital financial services. Insofar as it enables an authentication procedure based on independent factors, it ensures a high level of security, the subjective attribution of operations, and the protection of authentication credentials, in line with the highest standard recognised under European Union law. In this sense, digital identity infrastructures do not merely enable access to services, but also constitute a precondition for the traceability and contestability of algorithmic decision-making.

This framework makes clear that the eIDAS 2.0 Regulation provides the legal foundation of the trust upon which the technical resilience envisaged by the DORA Regulation is built. The argument advanced here is that this identity infrastructure may be further strengthened through the adoption of a Self-Sovereign Identity (SSI)[84] model based on Distributed Ledger Technology, thereby extending the legal foundation of digital identity into a fully-fledged ecosystem of distributed trust.

As recent developments in the computer science literature demonstrate[85], the combination of Self-Sovereign Identity and DLT makes it possible to reallocate the guarantee function from central authority to the distributed architecture of the ledger. This reallocation does not displace public authority, but rearticulates it through a legally framed technical architecture in which trust is redistributed. The functional validity of digital identity is no longer grounded exclusively in *ex lege* certification, being computed and cryptographically verified

[81] They constitute qualified electronic identification means, issued or recognised by the Member States, which enable users to create, store, and use digital identity credentials and electronic attribute attestations with full legal effect throughout the Union. The wallets are governed by Articles 5b-5i of the eIDAS 2.0 Regulation and are designed to ensure security, interoperability, user control, and mandatory acceptance by certain public and private entities, including those operating in the financial sector.

[82] This provision assigns to the wallets an infrastructural function of reliable identification, qualified authentication, and secure management of attributes, capable of supporting the subjective attribution of digital operations, non-repudiation, and the evidentiary effectiveness of transactions, in line with the requirements of operational continuity and access control laid down by the DORA Regulation.

[83] Pursuant to Article 4(30) of Directive (EU) 2015/2366 (PSD2), it "means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data".

[84] This expression refers to a model of digital identity in which the identity holder retains direct control over their credentials and identifying attributes, and is able to autonomously determine their creation, storage, and presentation to third parties, without relying on a central authority as the sole intermediary of identification. Within this model, the guarantee function of identity is not entrusted exclusively to a certifying authority, but is ensured by the technical architecture of the system and by cryptographic mechanisms that enable the verification of the authenticity and integrity of attestations, without prejudice to the need for legal recognition of the effects of the identity itself.

[85] A comprehensive elaboration of a Self-Sovereign Identity model based on Distributed Ledger Technology is proposed, for example, by A. DE SALVE, D. DI FRANCESCO MAESA, P. MORI, A. PUCCIA, L. RICCI, *A Multi-layer Trust Framework for Self-Sovereign Identity on Blockchain*, *Online Social Networks and Media*, vol. 37, 2023, pp. 1-12, where the trust function is anchored in a distributed architecture grounded in cryptographic mechanisms of verifiability, traceability, and selective control of attributes.

within the network[86]. Blockchain technology ensures the immutability and traceability of credentials, while Self-Sovereign Identity restores to the individual direct control over personal data, enabling a decentralised and transparent management of identity relationships between public and private actors[87].

The integration of the eIDAS 2.0 Regulation with SSI/DLT technologies therefore maximises the operational resilience of the European digital identity infrastructure by strengthening its security, transparency, and interoperability.

If eIDAS 2.0 provides the legal foundation of trust, blockchain represents its distributed technical implementation, capable of translating into computational terms the principles of authenticity, traceability, and non-repudiability that European law recognises as essential to the digital economy. From this perspective, the digital identity infrastructure itself acquires systemic relevance, since a concentration of identification and authentication functions in non-interoperable or insufficiently resilient solutions may constitute a Single Point of Failure, with consequences for the operational continuity of financial services and for dependencies on critical technology providers.

9. COMPUTATIONAL PROVISIONS AND ALGORITHMIC PRESCRIPTIONS IN THE INTEGRATION OF DLT AND SELF-SOVEREIGN IDENTITY

In light of the distinction between computational provisions and algorithmic prescriptions developed above (*supra* § 4.1), the integration of Distributed Ledger Technology and Self-Sovereign Identity marks a genuine qualitative shift in the form of digital regulation. In this context, the computational rule governing identity tends to evolve into an algorithmic rule of governance embedded within the technical infrastructure itself.

Under the traditional model, technology is confined to executing or attesting a legal norm while remaining external to it. Trust is delegated to a central authority that certifies identity and guarantees its validity, as is the case with systems such as SPID or CIE, where compliance is verified *ex post* and the rule remains separate from code. The combined use of Self-Sovereign Identity and DLT reverses this logic, as it transfers the guarantee function from central authority to the distributed architecture of the ledger. The validity of identities and attestations is no longer merely certified, but collectively computed and cryptographically verified within the

[86] More generally, the computer science literature has clarified that, within Self-Sovereign Identity models, the operational validity of digital identity is rendered verifiable through cryptographic mechanisms embedded in the system architecture. In particular, S. FERDOUS, F. CHOWDHURY, M. O. ALASSAFI, *In Search of Self-Sovereign Identity Leveraging Blockchain Technology*, in *IEEE Xplore*, n. 7, 2019, pp. 103059-103079, show how the authenticity, integrity, and validity of digital credentials are computed and verifiable within the network by means of distributed ledgers and cryptographic proofs, while clearly distinguishing the plane of technical verification from that of legal recognition.

[87] From a socio-institutional perspective, see F. WANG, P. DE FILIPPI, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, in *Frontiers in Blockchain*, n. 3, 2020, esp. Sections 4 and 5. The authors analyse SSI systems as trust infrastructures capable of fostering economic inclusion, cross-border portability of identity, and the reduction of power asymmetries, showing how the technical verifiability of attestations integrates with the legal recognition of digital identity.

network. The legal rule thus becomes incorporated into the technical infrastructure, transforming itself into a mechanism of automatic and verifiable implementation.

This transition – from a model based on the digitalisation of processes to one grounded in a computational infrastructure of trust – fully realises an algorithmic rule of governance consistent with the principles of resilience, traceability, and trust enshrined in European digital resilience law. In this sense, the transformation of the computational rule into an algorithmic rule of governance affects not only the modalities through which the norm is implemented, but also the conditions under which it is exercised and controlled, shifting regulatory attention towards the infrastructural preconditions that make supervision possible. By embedding the rule within the infrastructure itself, this model enables a form of supervision that operates not only on outcomes, but on the conditions of possibility of regulatory action.

10. BEYOND DATA-DRIVEN CYBER SUPERVISION: THE TRUST INFRASTRUCTURE

The structural dependence of data-driven supervision on the interoperability of algorithmic regulatory platforms, highlighted above (*supra* § 4), makes it possible to interpret the integration of blockchain within the regulatory frameworks established by the eIDAS 2.0 and DORA Regulations as the emergence of a genuine infrastructure of meta-supervision. This infrastructure is aimed at ensuring computational trust and institutional legitimacy for algorithmic mechanisms of market oversight. Where it is not possible to ascertain in real time the concrete impact of algorithms on supervisory decision-making, and where such verification remains confined to *ex post* control, the need arises for a technical safeguard capable of rendering that verification automatic, continuous, and objectively accessible.

It is from this perspective that Distributed Ledger Technology may respond to the deficit of transparency and reviewability inherent in algorithmic supervision, by introducing a form of "native" accountability that is intrinsic to the functioning of the infrastructure itself. DLT makes it possible to ground control not in the internal intelligibility of algorithmic processes, but in the immutable recording of the legally relevant evidence underlying supervisory decisions throughout the entire supervisory chain.

Within this configuration, blockchain is not intended to host data or algorithmic models as such, nor to replace the analytical systems employed by supervisory authorities. Rather, it operates as an immutability register of decisional traces, through the indelible preservation of the digital fingerprints (hashes)[88] of the rules and

[88] The term "hash" refers to the output of a cryptographic function that transforms a dataset of any size into a fixed-length string uniquely associated with that data, such that even a minimal alteration of the original information produces a radically different value. A hash does not allow the reconstruction of the content of the original data, but enables the verification of its integrity and non-alteration, functioning as a digital fingerprint of the information. In blockchain-based architectures, the hash performs a structural function. Each block incorporates the hash of the previous block, so that the ledger chain is cryptographically linked and any subsequent modification becomes immediately detectable. In this way, blockchain immutability does not derive from a legal prohibition or from centralised control, but from the cryptographic configuration of the ledger itself, which makes the integrity of data verifiable over time. For a

models applied. In this way, the traceability and verifiability of supervisory operations are ensured *ex ante* at the infrastructural level, making any modification, substitution, or update of the adopted models immediately detectable.

At the same time, the recording of the fingerprints of input data and of the exact moment at which an alert or recommendation is triggered allows the *ex post* reconstruction of the causal sequence of automated decisions. This makes it possible, for supervisory review purposes, to render intelligible the link between information, algorithmic processing, and supervisory intervention.

At a further level, DLT may be employed in the exercise of supervisory functions to record and digitally sign, in accordance with the standards set out in the eIDAS 2.0 Regulation, the chain of custody of digital evidence underpinning enforcement actions. This chain includes logs, reports, and supporting documentation. In this way, blockchain would provide a cryptographic basis capable of shielding such evidence from challenges relating to subsequent tampering or alteration, thereby directly affecting the conditions of legality and exercise of sanctioning powers.

It follows that, even without rendering algorithms technically explainable, DLT is capable of making the legal conformity of their operation verifiable. Each supervisory action thus becomes subject to *ex post* review based on technically non-manipulable records, capable of consolidating responsibility and legitimacy in the exercise of automated regulatory power. In this respect, DLT strengthens human oversight and institutional accountability to a degree that traditional centralised databases are unable to guarantee.

A further level of control thus emerges, in which the technical infrastructure, rather than serving merely as an operational support, becomes a direct object of regulation and verification. This shift marks the transition from data-driven cyber supervision to a genuine meta-supervision of the conditions under which public power is exercised.

11. FROM SOURCE CODE DISCLOSURE TO ALGORITHMIC SUPERVISORY TRANSPARENCY

The use of artificial intelligence algorithms by public administrations and independent supervisory authorities raises a central question concerning transparency when such systems are employed in the exercise of public functions and, for present purposes, in supervisory activities. It is well known that the Artificial Intelligence Regulation, while introducing detailed transparency obligations for providers and users of high-risk AI systems – including requirements relating to technical documentation and information to be made available

detailed analysis of the role of hashing as a tool for data integrity attestation and selective attribute disclosure in Self-Sovereign Identity models, see A. DE SALVE, A. LISI, P. MORI, L, RICCI, *Selective Disclosure in Self-Sovereign Identity Based on Hashed Values*, in *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)*, 2022, pp. 1-8, available at *ieeexplore.ieee.org/document/9913052*.

to competent authorities – does not recognise a general right of access to the source code of systems used in decision-making processes. It is nevertheless significant that Italian administrative case law anticipated this debate and adopted more far-reaching solutions. As early as March 2017, in two judgments of the Regional Administrative Court of Lazio[89], delivered in the well-known litigation concerning the algorithm used by the Italian Ministry of Education (MIUR) for teachers' mobility, the court recognised a right of access to the source code of the software employed for allocation procedures, qualifying it as a genuine form of digital administrative act[90].

This approach, although pioneering from a doctrinal perspective, has proven difficult to sustain in practice, as more recent scholarship has highlighted[91]. This is due not only to the need to protect the intellectual property rights of system providers, but also – and above all – to the high degree of technical complexity of source code, which often renders access devoid of genuine epistemic value and, in some cases, effectively unintelligible even for formally entitled parties. It follows that a conception of transparency understood as mere disclosure of source code is not, in itself, capable of ensuring effective accountability of algorithmic processes, leaving unresolved the core issue of the legal verifiability of automated administrative action.

Against this background, the solution proposed here leads to a different and innovative outcome. Source code may remain proprietary or inaccessible, and the law may move beyond the assumption that transparency must necessarily coincide with access to code. From this perspective, transparency ceases to be identified with the mere technical accessibility of the algorithmic tool and is instead recomposed as transparency of the supervisory function. Such transparency is entrusted to institutionally competent bodies endowed with the epistemic and evaluative tools necessary to scrutinise the legality, rationality, and proportionality of automated administrative action. In this sense, algorithmic supervisory transparency does not rest on the exposure of code, but on the existence of infrastructures capable of rendering supervisory action itself traceable, verifiable, and institutionally accountable.

12. A POSSIBLE NEW MODEL OF DIGITAL LEGITIMACY

The convergence between algorithmic accountability and distributed identity outlines the possibility of a new model of digital legitimation, one in which blockchain is not merely a technical data register, but a genuine infrastructure of meta-supervision. Once the DORA and eIDAS 2.0 Regulations are implemented within a unified DLT-based architecture through a Self-Sovereign Identity system, three distinct levels of techno-

[89] TAR Lazio, Rome, Section III-bis, judgments nos. 3742/2017 and 3769/2017.

[90] For a further discussion of these issues, see T. FAVARO, *Artificial Intelligence in Italian Public Administration: Challenges, Case Studies and Regulatory Perspectives*, above; see also M. B. ARMIENTO, *Pubbliche amministrazioni e intelligenza artificiale: Strumenti, principi e garanzie*, Editoriale scientifica, Napoli, 2024.

[91] For further discussion, see, inter alia, A. MITCHELL, D. LET, L. TANG, *AI Regulation and the Protection of Source Code*, in *International Journal of Law and Information Technology*, n. 4, 2023, pp. 283-301; A. TRONCI, *Le nuove frontiere della trasparenza nell'amministrazione algoritmica*, in *Federalismi*, n. 9, 2025, pp. 141-167, esp. at pp. 153 ff.

institutional application can be identified.

At the RegTech level, distributed technology enables supervised entities to automate compliance with regulatory obligations. Each supervisory operation may be digitally signed, in accordance with eIDAS identity standards, and anchored to the blockchain ledger, thereby ensuring traceability, integrity, and verifiability of decisions in line with the requirements of the DORA Regulation. In this perspective, blockchain operates as an infrastructure of compliance *by design*, in which the legal rule is incorporated into the very functioning of the technical system.

At the SupTech level, the same architecture enables distributed and verifiable oversight by supervisory authorities. External verification may be carried out through the validation of the hashes of recorded operations, ensuring a level of *ex post* transparency that centralised infrastructures are unable to provide. Blockchain thus becomes an instrument of algorithmic supervision capable of consolidating institutional trust through the automated verifiability of decision-making processes.

At the level of meta-supervision, blockchain ultimately assumes a genuinely institutional function. It no longer operates merely as a tool of efficiency or control, but takes the form of an infrastructure capable of enabling distributed supervision of the supervisory system itself, within which the exercise of power – whether human or algorithmic – is rendered transparent, traceable, and subject to verification.

Through the combined traceability of decisions (accountability) and the decentralised verifiability of subjects (identity), DLT thus makes it possible to restore transparency and accountability to algorithmic supervisory action. In this way, the public trust circuit – placed under strain by the delegation of regulatory and supervisory functions to automated systems – can be recomposed at the computational level, closing the conceptual loop from the "digitised process" to a fully-fledged "computational infrastructure of trust".

What emerges, therefore, is not merely a more efficient or technologically advanced form of supervision, but a redefinition of the conditions under which public power may be considered legitimate in a computational environment. In such a model, legitimacy no longer depends solely on the formal legality of decisions or on the opacity of technical expertise, but on the permanent possibility of verifying, contesting, and attributing responsibility for the exercise of regulatory power within the infrastructure itself.

Algorithmic supervision, as a result of this shift, may thus become not only data-driven, but also trust-driven: a system of computational meta-supervision in which even the controller is, in turn, subject to control through code. A chain of responsibility thereby emerges that mirrors the logic of the blockchain itself, in which each node participates in the generation of the decision and is correspondingly accountable for it.