BIBLIOTECA DI
STVDI VRBINATI

A CURA DI
ROSA PALAVERA, NICOLA PASCUCCI, CECILIA VALBONESI

SILENZIO, DIRITTO, DIRITTI



Urbino
University Press



BIBLIOTECA DI
STVDI VRBINATI

2

1506
UNIVERSITÀ DEGLI STUDI DI URBINO CARLO BO
UUP URBINO UNIVERSITY PRESS

La Collana Biblioteca di Studi Urbinati affianca la Rivista Studi Urbinati, che svolge un'intensa attività culturale e scientifica da quasi cento anni. La Collana accoglie opere individuali o collettanee di respiro monografico relative agli stessi ambiti scientifici della Rivista: Diritto, Economia, Scienze politiche, Sociologia.

A CURA DI
ROSA PALAVERA, NICOLA PASCUCCI, CECILIA VALBONESI

SILENZIO, DIRITTO, DIRITTI

SILENZIO, DIRITTO, DIRITTI
a cura di Rosa Palavera, Nicola Pascucci, Cecilia Valbonesi

Comitato di direzione
Ulrico Agnati, Marco Cangiotti (Direttore), Monica De Simone (Coordinatrice della redazione), Paolo Polidori, Cesare Silla

Comitato scientifico
Fei Anling (Università della Cina di Scienze Politiche e Giurisprudenza di Pechino), Roberta Cucca (Norwegian University of Life Sciences), Mauro Magatti (Università Cattolica del S. Cuore di Milano), Hans-Peter Müller (HU Berlin), Arpad Szakolczai (University of St. Gallen), Chiara Tenella Sillani (Università degli Studi di Milano), Bjørn Thomassen (Roskilde Universitet), Davide Ticchi (Università Politecnica delle Marche), Frederic Vandenberghe (IFCS-UFRJ), Romana Xerex (Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa)

Redazione
Monica De Simone (coordinamento), Rossella Iatomasi, Marco Pernarella, Francesca Zanetti

Progetto grafico
Mattia Gabellini

Referente UUP
Giovanna Bruscolini

In copertina
Vilhelm Hammershøi, *The tall windows*, Museum Ordrupgaard, Charlottenlund (Dk)

[Print] ISBN 9791257650087
[PDF] ISBN 9791257650063
[ePub] ISBN 9791257650070

Opera sottoposta a peer review secondo il protocollo UPI

Le edizioni digitali dell'opera sono rilasciate con licenza Creative Commons Attribution 4.0 - CC-BY, il cui testo integrale è disponibile all'URL: https://creativecommons.org/licenses/by/4.0/



Le edizioni digitali online sono pubblicate in Open Access su:
https://press.uniurb.it/index.php/UrbinoUP

© Gli autori per il testo, 2025, 2026
© Urbino University Press per la presente edizione
Pubblicato da: Urbino University Press | Via Saffi, 2 | 61029 Urbino
Sito web: https://uup.uniurb.it/ | e-mail: uup@uniurb.it

L'edizione cartacea del volume può essere ordinata in tutte le librerie fisiche e online ed è distribuita da StreetLib (https://www.streetlib.com/it/)

SOMMARIO

Ius tacere, ius tacendi 9
Rosa Palavera

Per non tacere il silenzio 15
Rosa Palavera, Nicola Pascucci, Cecilia Valbonesi

CAPITOLO I

Il silenzio come spazio normativo

Silenzio e potere politico in Roma antica 33
Margherita Frare

Misura e validazione della «diligenza organizzativa». Tra anomia, Stato post-regolatore, ordinamenti periferici 45
Eliana Greco

La comunicazione interna ed esterna dei modelli aziendali di organizzazione e controllo nella prevenzione del reato di intermediazione illecita e sfruttamento del lavoro 63
Filomena Pisconti

CAPITOLO II

Il silenzio del legislatore

Tra silenzi e dissimulazione: Gli inasprimenti di pena tramite la politica delle circostanze del reato 77
Gianluca Ruggiero

Extradition of Persons with Mental Disorders and the Related Administrative Dimension: A Comparative Perspective between Civil Law and Common Law Systems 95
Alessia Teresa Accoto

Blockchain and criminal protection of personal data: challenges and perspectives under GDPR and italian law 115
Carlotta Conversi

CAPITOLO III

Il silenzio delle spade

Restorative justice and supranational sources: an overview 129
Elena Mattevi

Gemelli diversi. La recente riforma spagnola in tema di giustizia riparativa non colma le distanze con il sistema italiano 145
Davide Bianchi

Reflections on the Legitimacy and Limits of EU Sanctions in the Context of International Criminal Law 179
Magdi Nicoletta Vecchiet

CAPITOLO IV

Il silenzio delle vittime

I percorsi riparativi nei casi di violenza contro le donne. 199
La narrazione come risposta al "silenziamento" della vittima fra dinamiche di reificazione e "ingiustizia epistemica"
Marta Lamanuzzi

Rumore bianco, le città sorgive e i centri di aiuto per le vittime di reato. 215
Donde hay musica no puede haber cosa mala
Ivan Cecchini

CAPITOLO V

Silenzi dietro le sbarre

Il "silenzio degli innocenti": infanzia reclusa. 267
Quali possibili strategie per tutelare chi non può difendersi?
Emma Tidu

La pena del silenzio: separazione e disumanizzazione.
Riflessioni dal film Il segreto dei suoi occhi di Juan Josè Campanella 297
Alberto Tortoroglio

BLOCKCHAIN AND CRIMINAL PROTECTION OF PERSONAL DATA: CHALLENGES AND PERSPECTIVES UNDER GDPR AND ITALIAN LAW

Carlotta Conversi

1. INTRODUCTION

The rapid diffusion of blockchain technology has profoundly altered the landscape of data governance, decentralization, and digital identity. Initially conceived as the infrastructure behind cryptocurrencies like Bitcoin, blockchain has since evolved into a multipurpose technology applied in finance, health, logistics, and, notably, personal data processing. Blockchain's core features – immutability, decentralization, and transparency – pose unique challenges to data protection regimes, particularly the European Union's General Data Protection Regulation (GDPR) and national criminal provisions such as Articles 167-bis and 167-ter of the Italian Data Protection Code (D.lgs. 196/2003, as amended by D.lgs. 101/2018).

Beyond its technical appeal, blockchain represents a paradigmatic test case for the adaptability of contemporary legal systems. The clash between distributed architectures and traditional models of accountability raises questions not only of regulatory compliance but also of the scope and effectiveness of criminal law as an instrument of last resort. In fact, blockchain highlights the limits of a legal order that presupposes identifiable actors, linear causation, and centralized control[1].

This introduction therefore situates blockchain within the broader debate on digital constitutionalism[2], informational self-determination, and the evolution of criminal enforcement in the age of decentralization. It suggests that the protection of personal data can no longer be understood solely through administrative and civil enforcement, but must also include a reflection on the boundaries and functions of criminal law. By expanding the scope of the introduction in this way, the article aims to frame blockchain not as a purely technical prob-

1 P. Hacker, I. Lianos, G. Dimitropoulos, S. Eich (eds.), *Regulating Blockchain. Techno-Social and Legal Challenges*, Oxford University Press, Oxford 2019.

2 E. Celeste, *Digital constitutionalism: a new systematic theorisation*, in International Review of Law, Computers & Technology 33 (2019) 76-99.

lem for compliance, but as a profound legal and philosophical challenge for the future of privacy and criminal justice.

While GDPR is widely recognized as the gold standard of privacy regulation globally[3], its principles of accountability, purpose limitation, data minimization, and the right to erasure appear fundamentally at odds with the technological structure of blockchain. For instance, the inability to modify or delete entries on a blockchain directly contradicts the right to be forgotten under Article 17 GDPR. This tension has prompted scholars to question the compatibility of blockchain with existing data protection laws[4].

Beyond civil and administrative consequences, violations of data protection norms can entail criminal liability under certain national legal frameworks. In Italy, Articles 167-bis and 167-ter of the Italian Data Protection Code, introduced by D.lgs. 101/2018, represent a selective and targeted penal protection of personal data, aimed at sanctioning specific harmful conduct beyond mere administrative non-compliance[5]. These provisions were designed to align Italian criminal law with the GDPR's enforcement regime while preserving proportionality and legality in criminal sanctions.

However, the application of such criminal norms in the context of blockchain remains ambiguous. The decentralized and transnational nature of blockchain systems raises complex questions regarding jurisdiction, intent, and the identification of responsible actors. Moreover, blockchain-based data processing often involves pseudonymous identifiers, further complicating the attribution of unlawful conduct and the imposition of penal consequences[6].

2. THE REGULATORY FRAMEWORK: GDPR AND THE ITALIAN DATA PROTECTION CODE

The European legal framework for the protection of personal data is primarily governed by the General Data Protection Regulation (GDPR), adopted in 2016 and enforced since May 2018. This regulation introduced a harmonized approach across the European Union, strengthening individuals' rights while imposing

3 P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, Cham 2017.

4 M. Finck, *Blockchains and Data Protection in the European Union*, in European Data Protection Law Review 4 (2018) 17-35.

5 G. Martiello, *La tutela penale dei dati personali: un'introduzione agli artt. 167, 167-bis e 167-ter del c.d. «codice della privacy»*, in disCrimen 1 (2022) 87-102.

6 A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Working Paper, 2015.

clear obligations on data controllers and processors. It aims to ensure transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity of personal data. The GDPR also affirms a wide array of data subject rights, such as access, rectification, erasure, and data portability, as well as providing mechanisms for redress and supervision through Data Protection Authorities.

Despite the GDPR's sophistication, it does not itself establish criminal sanctions. Instead, Article 84 of the GDPR explicitly leaves it to Member States to introduce penal consequences for particularly serious violations, provided these are effective, proportionate, and dissuasive. Thus, the question of criminal enforcement is inherently tied to national legislative discretion.

In Italy, this discretion was exercised through D.lgs. 101/2018, which modified the Italian Data Protection Code (D.lgs. 196/2003) to ensure alignment with the GDPR. Crucially, the Decree introduced and redefined several provisions aimed at reinforcing penal protection for privacy breaches. Article 167 of the Italian Data Protection Code targets unlawful data processing that results in tangible harm and is carried out with intent to gain or to cause injury. Article 167-bis expands criminal liability to the unauthorized processing of special categories of personal data, such as those concerning racial origin, political opinions, health, or sexual life, regardless of whether actual harm occurs. Article 167-ter, instead, penalizes the unlawful communication or dissemination of personal data that should be protected by specific technical or organizational safeguards.

These penal provisions reflect a selective criminalization approach, focused not on every regulatory breach but on conduct deemed socially dangerous or morally blameworthy. As Martiello notes, the intent behind these articles is to draw a clear line between administrative non-compliance and criminal wrongdoing, reserving the latter for the most serious threats to individual dignity and informational self-determination[7].

Yet, the application of these norms to blockchain-based systems remains uncertain. Italian criminal law, grounded in the principles of legality and strict interpretation, may struggle to accommodate emerging technologies that blur traditional legal categories, although this tension does not necessarily rule out an interpretation of existing provisions capable of addressing new technological contexts. The attribution of liability in decentralized systems is particularly problematic: identifying a data controller or processor – a fundamental prerequisite under both the GDPR and national criminal law – becomes elusive when data is managed collectively by pseudonymous or anonymous nodes across

7 G. Martiello, *La tutela penale dei dati personali*, cit.

jurisdictions. In this respect, the decentralized nature of blockchain directly challenges not only regulatory enforcement, but the basic conceptual underpinnings of criminal responsibility in privacy law[8].

3. BLOCKCHAIN'S STRUCTURAL TENSIONS WITH DATA PROTECTION PRINCIPLES

Blockchain technology, by design, introduces systemic tensions with the fundamental principles of data protection law. As a distributed ledger system, blockchain ensures that data entered into the network is immutable, tamper-resistant, and replicated across numerous nodes. This structure, while enhancing security and trust in decentralized environments, presents serious challenges for the implementation of core privacy rights, particularly under the GDPR.

One of the most prominent conflicts arises from the principle of data minimization and the right to erasure. Article 5(1)(c) of the GDPR mandates that personal data should be «adequate, relevant and limited to what is necessary», while Article 17 of the GDPR confers on individuals the «right to be forgotten». These provisions require that data controllers be able to delete or modify personal data upon request or when the lawful basis for processing no longer applies. However, in a blockchain environment, data is irreversibly written into the ledger. Although some architectural solutions – such as storing only hashes or using off-chain storage – have been proposed to mitigate this issue, they often fall short of fully satisfying the GDPR's requirements[9].

Moreover, the decentralization inherent in blockchain disrupts the traditional accountability model of data protection law. GDPR relies on the clear identification of a data controller and, where applicable, a processor. These roles carry specific responsibilities, including responding to data subject requests, ensuring lawful bases for processing, and notifying authorities in case of data breaches. In public or permissionless blockchains, however, there may be no identifiable or legally responsible entity orchestrating the processing. Instead, data is collectively validated and stored by multiple, often anonymous, nodes.

8 M. Finck, V. Moscon, *Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0*, in IIC – International Review of Intellectual Property and Competition Law 50 (2019) 77-108.

9 M. Finck, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, European Parliamentary Research Service – Scientific Foresight Unit (STOA), Brussels 2019.

This fragmentation undermines enforcement efforts and raises complex questions about how criminal or administrative responsibility can be assigned[10].

Another key issue is the problem of pseudonymity. Blockchain networks typically allow users to interact through cryptographic keys rather than real names, creating a pseudonymous environment. While this enhances user privacy in theory, it also hinders legal authorities from identifying wrongdoers, especially in cross-border contexts. The GDPR defines personal data broadly to include «any information relating to an identified or identifiable natural person» (Art. 4(1) GDPR). As such, even a blockchain address can qualify as personal data if it can be linked – directly or indirectly – to an individual[11]. This broad interpretation imposes regulatory obligations on actors who may not even consider themselves part of a formal data processing chain.

These structural tensions are even more acute when viewed through the lens of criminal law. Unlike civil or administrative liability, criminal sanctions require higher thresholds of proof, including *mens rea* (criminal intent) and a clearly defined unlawful act. In the blockchain context, proving intent, identifying actors, and demonstrating unlawful data processing is exceptionally difficult. A node operator may not be aware that the data stored in a block is personal or sensitive; participants may be acting according to a consensus algorithm rather than with individual purpose. This undermines the foundational criminal law principles of culpability and personal responsibility[12].

4. CRIMINAL LIABILITY AND THE ITALIAN ARTICLES 167-BIS AND 167-TER

The Italian legal system provides for criminal liability in the context of data protection violations through specific provisions embedded in the Italian Data Protection Code, as amended by D.lgs. 101/2018. Among these, Articles 167-bis and 167-ter represent key instruments for penal enforcement, especially when sensitive personal data is processed or disseminated unlawfully.

Article 167-bis of the Italian Data Protection Code criminalizes the unlawful processing of special categories of personal data, such as those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health status, or sexual orientation. What is notable about this provision is that it does

10 P. Hacker, I. Lianos, G. Dimitropoulos, S. Eich (eds.), *Regulating Blockchain*, cit.

11 M. Finck, *Blockchains and Data Protection in the European Union*, cit.

12 A. Wright, P. De Filippi, *Decentralized Blockchain Technology*, cit.

not require actual harm to be demonstrated. The mere violation of obligations imposed by law or regulation, when committed without appropriate authorization or a valid legal basis, is sufficient to establish criminal liability. This reflects a legal recognition that the very act of misusing sensitive data may endanger human dignity and informational autonomy, even in the absence of economic or psychological damage[13].

Article 167-ter of the Italian Data Protection Code, in turn, penalizes the unlawful communication or dissemination of personal data that is protected by specific technical or organizational security measures. This applies in situations where personal information – such as biometric data, health records, or data subject to profiling – is shared or exposed without compliance with legal safeguards. The aim is to address cases where the mere loss of confidentiality may pose significant risks to data subjects, irrespective of how the data is ultimately used.

Both provisions embody a selective criminalization model, grounded in the principles of *ultima ratio* and proportionality. Italian legislators have refrained from broadly criminalizing all forms of GDPR violations. Instead, penal sanctions are reserved for conduct that is considered particularly serious from a social or ethical standpoint. However, this approach reveals its limitations when applied to decentralized technologies such as blockchain.

These difficulties compound the identification problem already noted above: in pseudonymous, multi-node systems, no single actor typically fits the figure of a data controller or processor on which both the GDPR and Italian criminal law rely. As Finck and Moscon have argued, blockchain challenges the traditional legal concepts of control, purpose limitation, and accountability that underpin data protection enforcement[14].

A related complication concerns the fault requirement discussed earlier: since participation in a validation process is typically algorithmic rather than the product of individual decision-making, establishing that a node operator or developer acted with intent or negligence is correspondingly difficult.

Furthermore, jurisdictional concerns are amplified in decentralized settings. Unlike the GDPR, whose Article 3 asserts a broad extraterritorial reach, Italian criminal law adheres more strictly to territorial principles. This poses challenges when blockchain nodes or actors are located abroad. Although mutual legal assistance mechanisms and international cooperation can address some of these

13 G. Martiello, *La tutela penale dei dati personali*, cit.

14 M. Finck, V. Moscon, *Copyright Law on Blockchains*, cit.

gaps, the diffuse and transnational nature of blockchain systems continues to frustrate effective enforcement.

At this stage, the general principles of criminal law become relevant correctives. The notion of *concorso di cause*, as discussed under Article 40 of the Italian Penal Code, allows liability to be shared when multiple factors contribute to a harmful outcome. This doctrine, traditionally employed in cases of complex causal chains, could be adapted to blockchain, where the unlawful result is often the cumulative effect of various algorithmic and human contributions[15]. Similarly, the criteria of territoriality contained in the opening provisions of the Italian Penal Code (Articles 6-10) provide interpretive tools to extend jurisdiction when part of the unlawful conduct or its effects occur on Italian soil[16].

By explicitly referencing these principles, courts and scholars can demonstrate that classical criminal categories – such as causation, territoriality, and culpability – still offer valuable interpretive guidance when applied to emerging digital infrastructures. Such a move would not only give more conceptual breadth to privacy-related criminal law but also underline the continuity between traditional penal doctrines and new technological challenges. In this perspective, blockchain becomes not merely a disruptive anomaly, but a testbed for the resilience of general principles of criminal law.

5. COMPARATIVE REFLECTIONS: U.S. APPROACHES TO BLOCKCHAIN AND PRIVACY VIOLATIONS

While the European Union has developed a comprehensive framework for data protection centered on the GDPR, the United States adopts a sectoral and fragmented approach, lacking a unified federal privacy statute. This divergence is especially relevant when comparing how each system addresses blockchain-based privacy violations and whether criminal enforcement plays a meaningful role in safeguarding personal data.

In the United States, data protection is governed by a patchwork of federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA), alongside state-level legislation like the California Consumer Privacy Act (CCPA). None of these laws, however, systematically

15 F. Mantovani, *Diritto penale. Parte generale*, VII ed., Cedam, Padova 2011.

16 G. Marinucci, E. Dolcini, G.L. Gatta, *Manuale di diritto penale. Parte generale*, VI ed., Giuffrè, Milano 2017.

regulate blockchain technologies, nor do they establish strong criminal penalties for general privacy violations. Enforcement is typically administrative or civil in nature, led by agencies such as the Federal Trade Commission (FTC).

Nevertheless, certain federal laws have been used in criminal prosecutions involving digital privacy breaches. The Computer Fraud and Abuse Act (CFAA), for example, provides criminal sanctions for unauthorized access to protected computers, which has been applied in cases involving data scraping or digital trespass. However, the CFAA was not designed to address decentralized architectures or blockchain-specific behavior. As such, its applicability to blockchain-related privacy issues is limited and often controversial[17].

In contrast to the GDPR's principle of accountability, which imposes positive obligations on data controllers and processors, U.S. law tends to focus on the prevention of harm through ex post remedies. Privacy enforcement is often triggered only after a breach has occurred and actual damage can be shown. This reactive posture is ill-suited to blockchain environments, where data, once recorded, cannot be modified or erased. Immutable records on blockchain systems challenge the very foundation of consent-based privacy protection, since users may not anticipate the long-term consequences of recording personal information on a permanent ledger.

Moreover, the decentralized nature of blockchain exacerbates enforcement difficulties. In the U.S., jurisdiction depends heavily on the location of servers, users, or companies. Blockchain systems, by their very nature, operate across jurisdictions and may involve anonymous participants who are impossible to locate or prosecute. This raises practical barriers for law enforcement, especially when blockchain is used for illicit activities such as identity theft, doxxing, or unauthorized data publication.

From a comparative perspective, both the U.S. and EU face similar challenges when dealing with blockchain's incompatibility with traditional privacy concepts. However, the EU's attempt to reconcile blockchain with GDPR principles – through technical guidelines, regulatory sandboxes, and legal interpretation – demonstrates a more proactive commitment to privacy-by-design. By contrast, U.S. criminal law appears less equipped to engage with the nuances of distributed ledger systems in a data protection context.

Still, recent developments in U.S. state law signal a potential shift. Laws such as the New York SHIELD Act and the Washington Privacy Act introduce higher standards for data security and create more stringent reporting require-

17 O.S. Kerr, *Computer Crime Law*, II ed., Thomson/West, St. Paul 2009.

ments. Though primarily civil, these laws could lay the groundwork for future criminal enforcement mechanisms adapted to decentralized technologies.

6. THE ROLE OF TECHNOLOGY-NEUTRAL CRIMINAL LAW AND FUTURE CHALLENGES

The challenges posed by blockchain to the criminal protection of personal data raise a broader question: to what extent can criminal law remain effective in a technologically evolving environment without undergoing structural transformation? This dilemma is especially relevant for legal systems like Italy's, which are rooted in principles of legality, typicity, and personal culpability. These foundations, while essential to safeguarding individual liberties, may limit the flexibility of the law to confront emerging, non-traditional forms of harm and accountability.

One of the prevailing responses to this dilemma is the concept of technology-neutral regulation. Technology-neutrality suggests that laws should be drafted in a way that applies across technological contexts, focusing on behavior and outcomes rather than the technical means used. In theory, this approach allows legal norms – including criminal statutes – to endure despite rapid innovation. In practice, however, such neutrality can prove illusory when the assumptions underlying legal categories no longer align with technical realities[18].

Criminal law in the context of data protection exemplifies this tension. Provisions like Articles 167-bis and 167-ter of the Italian Data Protection Code are formally technology-neutral but assume a centralized model of data governance, identifiable actors, and a linear causality between unlawful conduct and harm. These assumptions are incompatible with blockchain systems, where data is processed in a decentralized, multi-node environment, and control is often algorithmically distributed. As a result, even when a blockchain-based action clearly infringes on data subject rights – such as recording sensitive personal data without consent – the path to establishing criminal responsibility remains legally uncertain.

Another problem lies in the application of traditional concepts such as "unlawful processing" or "unauthorized communication" in the context of smart contracts and automated consensus mechanisms. The automated nature of these systems complicates the attribution of intent (*mens rea*), a cornerstone of criminal responsibility. If a privacy breach occurs due to a flaw in a smart

18 R. Brownsword, *Law, Technology and Society. Re-imagining the Regulatory Environment*, Routledge, Abingdon 2019.

contract or an automated process without human intervention, can criminal liability be assigned, and to whom? These questions illustrate how automation and decentralization strain classical legal doctrines.

Moving forward, lawmakers and courts may need to consider new models of liability and enforcement that reflect the realities of decentralized digital infrastructures. One possibility is the development of functional analogues to the figure of the data controller, adapted to blockchain environments. This could include attributing responsibility to entities or individuals who initiate or design blockchain applications, or who have the power to influence technical parameters that affect data processing. Another avenue is the creation of a collective or shared liability framework, in which responsibility is distributed among network participants based on their roles and capacities[19].

From a normative perspective, legislative reforms could explicitly recognize blockchain-specific categories of responsibility, introducing presumptions of liability for developers and validators where compliance duties are structurally unavoidable. For example, blockchain architects who design smart contracts that inherently process personal data could be required to integrate privacy-by-design measures, with criminal liability arising only in cases of deliberate circumvention or reckless omission[20]. Furthermore, amendments to Articles 167-bis and 167-ter of the Italian Data Protection Code could clarify how unlawful dissemination or unauthorized processing should be interpreted in decentralized contexts, ensuring that the criminal law remains both effective and proportionate.

Such proposals would align criminal enforcement with the principle of technological neutrality[21], while adapting it to the structural peculiarities of distributed ledger systems. In this sense, criminal law could evolve toward a risk-based and forward-looking approach, where the allocation of responsibility reflects both the preventive duties of blockchain designers and the residual accountability of network participants. This would avoid a merely symbolic penal protection and ensure that criminal sanctions operate as an *ultima ratio*, complementing – but not duplicating – the administrative mechanisms provided under the GDPR[22].

19 M. Finck, V. Moscon, *Copyright Law on Blockchains*, cit.

20 A. Wright, P. De Filippi, *Decentralized Blockchain Technology*, cit.

21 R. Brownsword, *Law, Technology and Society*, cit.

22 P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, cit.

7. CONCLUSION

The emergence of blockchain technology challenges the foundational assumptions of data protection law, particularly when examined through the lens of criminal liability. Designed to ensure transparency, immutability, and decentralization, blockchain disrupts conventional legal models that rely on centralized control, identifiable actors, and clear lines of accountability. As this paper has shown, the friction between blockchain and the European data protection regime – anchored in the GDPR and national implementations such as the Italian Data Protection Code – is not merely technical but structural and conceptual.

Articles 167-bis and 167-ter of the Italian Data Protection Code were introduced to provide targeted criminal sanctions for serious privacy violations, especially those involving sensitive personal data or unlawful dissemination. However, their effective application presupposes a legal environment that blockchain resists: one in which actors are known, actions are traceable, and intent can be established. In decentralized networks governed by consensus algorithms and pseudonymity, these conditions often fail to materialize.

Comparative analysis with the United States reveals that while criminal enforcement of privacy violations is generally limited under U.S. law, the same structural challenges are evident. Legal frameworks on both sides of the Atlantic remain ill-equipped to address the risks posed by blockchain-based data processing, particularly in public and permissionless systems. Yet, the European approach, with its focus on data subject rights and proactive regulatory engagement, may offer a more promising foundation for future reforms.

Looking ahead, the development of technology-neutral legal principles is essential but insufficient on its own. Legislators, courts, and regulatory authorities must engage in a deeper reconceptualization of responsibility, liability, and enforcement in the age of distributed digital infrastructures. This could involve redefining legal roles within decentralized systems, introducing shared or functional accountability, and adopting risk-based enforcement mechanisms that reflect the realities of blockchain governance.

In parallel, legal actors must be equipped with the knowledge and technical understanding necessary to interpret blockchain-based conduct through a criminal law lens. Without such efforts, the penal protection of personal data risks becoming symbolic – asserting rights and prohibitions that cannot be effectively enforced.