Assessing the Effectiveness of Compliance Programs Through the Use of the Metaverse and Blockchain

Nikos Passas[1,*] and Fabio Coppola[2]

[1]School of Criminology and Criminal Justice, Northeastern University, USA

[2]University of Salerno, Italy

Abstract: This paper examines how blockchain technology and the Metaverse can address persistent challenges in corporate compliance, with a focus on mitigating *criminogenic asymmetries*—such as regulatory arbitrage and opacity in cross-border transactions—through decentralized, transparent solutions. By contrasting the U.S. and Italian legal frameworks, we highlight the limitations of retrospective compliance evaluations and propose blockchain-enabled innovations, including immutable audit trails, smart contracts for automated enforcement, and Decentralized Autonomous Organizations (DAOs) to decentralize governance and embed compliance into protocol design. The Metaverse offers a simulated environment for stress-testing compliance protocols against emerging risks, while criminological theories (e.g., global anomie, legal-illegal interfaces) contextualize regulatory gaps in digital economies. We argue that DAOs, as digital-native entities, could revolutionize compliance by replacing hierarchical oversight with algorithmic governance, though challenges like jurisdictional fragmentation and identity verification persist. The study underscores the need for adaptive regulatory frameworks to harness these technologies while balancing transparency, accountability, and privacy.

Keywords: Regulatory arbitrage, criminogenic asymmetries, cross-border opacity), blockchain solutions, Decentralized Autonomous Organizations (DAOs), algorithmic governance, compliance automation, Metaverse compliance testing, behavioral analytics), Global Anomie, deregulation, virtual economies), "lawful but awful" practices, AI-Driven Compliance.

1. INTRODUCTION

The past three decades have witnessed a transformative shift in corporate compliance[1]—from reactive legal measures to proactive, technology-driven models. This evolution, marked by milestones such as the U.S. Federal Sentencing Guidelines for Organizations (1991), Italy's Legislative Decree No. 231/2001, and the UK Bribery Act (2010), reflects a broader trend toward embedding self-regulatory mechanisms into corporate governance. Today, compliance programs increasingly leverage digital monitoring and AI-enhanced auditing, signaling a new phase in crime prevention.

Corporations now engage in compliance through three primary approaches:

- **Enforced self-regulation**, where binding rules are imposed with sanctions for non-compliance;
- **Encouraged self-regulation**, offering incentives (e.g., sanction mitigation) for adopting compliance programs;
- **Voluntary self-regulation**, guided by non-binding soft-law standards.

This paper examines how AI and the Metaverse can enhance compliance program effectiveness by enabling real-time simulation testing and risk assessment. While prior research has explored compliance models in isolation, this study adopts a comparative approach, analyzing the U.S. (common law) and Italian (civil law) frameworks to identify shared challenges and opportunities for technological integration. By doing so, it seeks to address a critical gap: how emerging technologies can bridge the divide between theoretical compliance standards and practical implementation.

The analysis proceeds in three parts. First, it compares the structural and operational differences between the U.S. and Italian models. Second, it evaluates persistent challenges in compliance enforcement. Finally, it explores the potential of AI-driven simulations and Metaverse environments to revolutionize compliance training, monitoring, and testing—offering a pathway to more adaptive and resilient systems.

2. THE ITALIAN APPROACH TO CRIMINAL COMPLIANCE

The framework established by the Italian legislator for corporate criminal liability requires that corporate

*Address correspondence to this author at the School of Criminology and Criminal Justice, Northeastern University, USA;
E-mail: n.passas@northeastern.edu

[1]In this paper, we will refer exclusively to "criminal compliance", meaning the set of rules aimed at preventing corporate crimes.

E-ISSN: 1929-4409/25

offences be committed in the corporation's interest or to its advantage and that the corporation be found to have engaged in organizational fault. It is precisely in relation to this latter requirement that the role of criminal compliance becomes relevant.

Corporations are required to adopt preventive measures to mitigate the risk of corporate crimes through a structured process of risk assessment and risk management. If a company has adopted and effectively implemented a compliance program, it cannot be held liable for an offence committed in its interest or to its advantage. Conversely, if the corporation has failed to properly structure itself to prevent the commission of the crime, it will be deemed to have engaged in organizational fault and will be sanctioned for the offence.

Thus, in the Italian legal system, corporate culpability serves as a foundational prerequisite for liability in cases of corporate crime, rather than merely functioning as a mitigating factor during sentencing (Fiorella, 2016; Forti, 2012; Gargani, 2002; Manes, 2021; Paliero & Piergallini, 2006; Mongillo, 2023).

3. THE U.S. APPROACH TO CRIMINAL COMPLIANCE

In the U.S. legal system, corporate criminal liability operates independently of criminal compliance; consequently, the degree of corporate culpability does not constitute a foundational element of liability. Instead, criminal compliance plays a fundamental role within a carrot-and-stick strategy (Coffee, 1990).

On one hand, corporate liability arises regardless of the company's preventive efforts, as the mere occurrence of a corporate crime is considered sufficient to establish liability.

On the other hand, criminal compliance is crucial during the sentencing phase. If a corporation has adequately implemented preventive measures to mitigate the risk of the crime that was ultimately committed, the penalties imposed on the company may be significantly reduced. This approach reflects the U.S. system's intent to incentivize corporate compliance by granting substantial sentencing reductions to organizations that have proactively adopted and enforced effective compliance programs.

For instance, in the Wells Fargo scandal, despite internal compliance mechanisms, the company faced significant penalties due to fraudulent practices in account creation. The effectiveness of compliance programs remains a key determinant in sentencing outcomes.

While both legal systems recognize compliance programs as mitigating factors, the U.S. system penalizes corporate offenses regardless of preventive efforts, whereas Italy conditions liability on the absence of effective compliance structures.

4. SIMILARITIES AND DIFFERENCES IN CRIMINAL COMPLIANCE BETWEEN THE U.S. AND ITALY

From the brief description above, a fundamental difference in the approach to criminal compliance immediately emerges. In the U.S. legal system, compliance represents the benevolent side of the criminal law framework, incentivizing corporations to actively engage in the prevention of corporate crimes. In return, should such offences occur, companies that have implemented effective compliance measures are granted substantial sentencing reductions.

In contrast, under Italian law, a corporation may be held liable for corporate crimes only if it has failed to implement the necessary preventive safeguards or if the compliance measures in place are deemed ineffective.

Despite this significant distinction, there are also notable similarities. In both legal systems, the adoption of effective compliance programs provides substantial sanction-related benefits for corporations. In the U.S., it results in sentence mitigation, while in Italy, it can lead to complete exoneration from liability.

Moreover, in both legal systems, for a corporation to benefit from compliance-related advantages, its preventive program must be effective—that is, it must be specifically designed to address the criminal risks inherent in the corporate environment and must not be a mere window-dressing effort.

To define the requirements of an effective compliance program, the U.S. legal system has provided specific guidelines, identifying key pillars that corporations must adhere to in order to demonstrate the adoption of a robust preventive framework against corporate crimes.

The U.S. Sentencing Commission outlines seven key requirements for an effective compliance program, including oversight mechanisms, employee training, and internal reporting channels. In more detail, Chapter

8, Section B, Paragraph 2 of the U.S. Sentencing Commission Organizational Guidelines establishes the following:

"(a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (b)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

(1) exercise due diligence to prevent and detect criminal conduct; and

(2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offence does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

(b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:

(1) The organization shall establish standards and procedures to prevent and detect criminal conduct.

(2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

(B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

(C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.

(3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

(4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.

(5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

(6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

(7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process."

In this regard, the U.S. system appears to differ from the Italian framework, as Legislative Decree No. 231/2001 provides more limited guidance on assessing the effectiveness of compliance programs. Specifically, the decree merely requires that the organization:

- Adopt organizational and management models suitable for preventing offences of the type that has occurred;
- Establish a supervisory body responsible for overseeing the functioning and observance of the compliance models, ensuring their continuous updating, and endowed with autonomous powers of initiative and control;
- Implement an effective sanctioning system to penalize violations of the corporate compliance model.

Furthermore, the content of compliance programs must:

a) Identify the activities within which offences could be committed;

b) Establish specific protocols to plan the formation and implementation of the company's decisions concerning the crimes to be prevented;

c) Define financial resource management methods suitable for preventing the commission of offences;

d) Provide reporting obligations to the body responsible for supervising the functioning and observance of the compliance program;

e) Introduce a disciplinary system capable of sanctioning non-compliance with the measures outlined in the model" (Art. 6, Legislative Decree No. 231/2001).

We argue that the difference between the two systems is more apparent than real. While it is true that the U.S. Guidelines provide more specific criteria for assessing the effectiveness of compliance programs, both models ultimately face the same fundamental challenges. A major challenge in both systems is the retrospective nature of compliance evaluation, leading to potential hindsight bias in determining program effectiveness

The first critical issue concerns the ex-post assessment of a compliance program's effectiveness, meaning that its evaluation occurs only after the commission of an offence. This type of assessment is inherently prone to hindsight bias: if a crime was committed despite the existence of a compliance program, this is often taken as evidence that the program was ineffective (Forti, 2012).

The second, closely related issue pertains to the vagueness of the criteria intended to guide judicial discretion in evaluating compliance programs. The broad requirements set out in the U.S. Guidelines or Legislative Decree No. 231/2001 do not provide corporations with a sufficient degree of legal certainty regarding whether their compliance measures will be deemed effective.

In Italy, this uncertainty has led to corporate disaffection toward preventive compliance programs, as the substantial organizational and financial efforts invested in compliance are not supported by a presumption of effectiveness. As a result, corporations lack reasonable predictability as to whether their compliance framework will qualify them for the legal benefits granted under both systems to entities that have adequately structured themselves to prevent corporate crimes (Mongillo, 2011).

Table 1: Below Summarises the Differences between the Two Systems.

Aspect	U.S. System	Italian System
Liability Basis	Corporations liable regardless of compliance	Liability depends on compliance effectiveness
Compliance Role	Primarily affects sentencing	Determines liability itself
Guidance Detail	Extensive guidelines from USSC	General principles under Legislative Decree 231/2001

For these reasons, we will now proceed with an analysis of the core activities involved in the development of a compliance program, evaluating the potential impact of AI systems on these processes and, finally, exploring the role of the Metaverse in conducting a virtual simulation of the effectiveness test for compliance programs.

5. THE CORE FRAMEWORK OF A CRIMINAL COMPLIANCE PROGRAM

In constructing the essential framework of an effective compliance program, three fundamental components must be identified: a meticulous risk assessment phase, a comprehensive set of preventive policies (risk management), and a robust system of oversight and enforcement.

Phase 1: Risk Identification & Assessment

A corporation must first conduct a thorough self-evaluation to identify and assess the specific risks of corporate crime inherent in its operational environment and business activities. For instance, a corporation that interacts predominantly with public officials is naturally more exposed to corruption-related offences. Conversely, a company operating in the betting sector faces heightened risks of money laundering and tax evasion, while a pharmaceutical company would focus on regulatory compliance for drug safety.

This preliminary phase is crucial to ensuring the overall effectiveness of a compliance program. Only if the corporation systematically identifies and assesses all potential risks associated with its business activities can it implement a set of preventive measures tailored to mitigate those risks effectively.

Phase 2: Implementation of Preventive Policies

Once the corporation has determined which offences are most likely to occur and the mechanisms through which they could be committed, it must establish a structured framework of internal regulations aimed at preventing their commission. In practical terms, this involves defining precise guidelines on how employees and representatives should conduct themselves in high-risk areas to preempt illicit conduct. In the aforementioned examples, the compliance program would set out specific protocols governing interactions with public officials to prevent corruption offences, while also instituting rigorous financial transaction controls to mitigate risks related to money laundering.

The implementation of clear, structured protocols that align with the organization's best practices not only serves a preventive function but also enhances the efficiency of corporate procedures and strengthens employees' awareness of compliance obligations.

Phase 3: Oversight & Enforcement

Finally, the corporation must establish mechanisms for effective oversight and enforcement of its internal regulations. This includes disciplinary measures designed to ensure compliance with preventive policies and to sanction any violations thereof.

In the subsequent section of this paper, we will examine the potential contributions of artificial intelligence to each of these foundational pillars of a compliance program.

6. THE DEVELOPMENT OF DIGITAL COMPLIANCE

The advancement of artificial intelligence (AI) and digital compliance holds significant promise for corporate compliance frameworks, particularly furnishing three key benefits (Gullo, 2023):

a) Enhanced Crime Risk Assessment (e.g., Fraud Detection Using Machine Learning)

Machine learning can play a pivotal role in assisting corporations in the development of more effective compliance programs. The implementation of algorithmic models ensures a more precise collection and analysis of corporate data, thereby enabling a more refined and tailored assessment of crime-related risks within a specific business context. By leveraging ML-driven analytics, organizations can achieve a more accurate and dynamic understanding of the legal and regulatory threats they face, ultimately strengthening the risk assessment process.

b) Automated Internal Monitoring (e.g., AI-Driven Financial transaction Audits)

The digitalization of internal procedures and protocols significantly enhances oversight while also automating the identification of misconduct and the activation of preventive measures. For instance, the automation of financial transactions can serve as a safeguard against non-compliant payments by preemptively blocking transactions that contravene internal policies and regulatory standards.

Furthermore, the digitalization of corporate functions facilitates a more effective evaluation of the actual

implementation of preventive compliance models. On one hand, AI-driven systems can autonomously enforce compliance measures, reducing reliance on human intervention. On the other hand, AI-powered data analysis provides a more reliable and comprehensive mechanism for monitoring compliance effectiveness, surpassing traditional human oversight in terms of accuracy and efficiency.

c) Predicting Compliance Testing Programs (e.g., Forecasting Compliance Failures)

One of the most debated yet potentially transformative applications of AI in corporate compliance is its ability to predict corporate crimes and assess the effectiveness of preventive measures. This prospect inevitably evokes comparisons with the 2002 Hollywood film Minority Report, in which AI-driven predictive technology anticipates individual behaviors, identifies crimes before their commission, and enables law enforcement to intervene preemptively. However, while the notion of predictive justice raises significant ethical and legal concerns, corporate compliance could serve as a promising field for testing predictive models within a controlled and regulated framework (Burchard, 2020).

Nevertheless, reservations regarding reliance on algorithmic predictive capabilities are well-documented. A primary concern is the so-called black box nature of AI decision-making, which renders its reasoning opaque and difficult to scrutinize. Moreover, AI-driven compliance systems are susceptible to discriminatory biases—flaws that are unacceptable when exhibited by human decision-makers and arguably even more concerning when embedded in automated processes (Nisco, 2022).

Additionally, the prospect of fully digitalized compliance frameworks in Europe must be reconciled with the principles enshrined in the General Data Protection Regulation (GDPR) and the labor rights framework. A compliance model that entails near-continuous monitoring of employees' activities for the purpose of identifying and preventing corporate crimes before they occur would necessitate a careful balancing of regulatory objectives with fundamental rights, particularly in relation to privacy and data protection (Morgante & Fiorinelli, 2022). While AI improves compliance effectiveness, regulatory constraints like GDPR impose limitations on continuous employee monitoring, requiring a balance between enforcement and privacy rights.

6.1. The Role of Blockchain in Corporate Compliance

While blockchain is widely recognized for its ability to enhance compliance through immutable record-keeping, its potential extends far beyond this function. Emerging applications include real-time compliance monitoring, automated enforcement mechanisms, and the integration of decentralized autonomous organizations (DAOs) into corporate governance. Additionally, blockchain-based compliance models must address new financial risks, particularly those posed by cryptocurrency transactions and the potential for illicit financial flows.

6.2. Blockchain for Real-Time Compliance Monitoring

Traditional compliance frameworks rely on periodic audits and retrospective assessments, which may fail to detect violations in real time. Blockchain technology enables continuous, transparent monitoring of compliance obligations by leveraging decentralized ledger technology (DLT) to track corporate activities as they occur.

For example, regulatory authorities and auditors can be granted permissioned access to private or consortium blockchains, allowing them to monitor transactions, supply chains, and contractual obligations in real time (Zhao *et al*., 2022). In financial services, blockchain-based compliance systems have been proposed to automate Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements by validating identities and detecting suspicious transactions dynamically (Fang *et al*., 2023). These solutions reduce reliance on manual oversight and enhance regulatory effectiveness.

Moreover, blockchain-enabled Internet of Things (IoT) applications can be integrated into compliance programs to ensure regulatory adherence in industries such as pharmaceuticals, where real-time monitoring of supply chain integrity is critical (Casino *et al*., 2019). Also, cryptographic transparency (e.g., zero-knowledge proofs) reconciles privacy with AML/KYC requirements, making illicit flows traceable without exposing sensitive data. Such implementations improve transparency and reduce corporate liability by demonstrating proactive compliance measures.

6.3. Smart Contracts for Automated Compliance Enforcement

Smart contracts—self-executing contracts with pre-defined rules encoded on a blockchain—offer

significant potential for automating compliance enforcement and penalties. These contracts can be programmed to automatically enforce regulatory requirements, mitigating risks associated with human error and fraudulent activities.

For instance, in the financial sector, smart contracts can enforce tax compliance by withholding funds for tax obligations before transactions are executed (Cong & He, 2019). Similarly, in corporate governance, smart contracts can ensure adherence to ethical sourcing regulations by releasing payments only when verified compliance conditions—such as certification from third-party auditors—are met (Savelyev, 2017).

Regulatory agencies have also explored using blockchain-based smart contracts to enforce sanctions and embargoes by restricting non-compliant transactions at the protocol level (Wright & De Filippi, 2015). This approach ensures that entities engaged in high-risk activities cannot circumvent legal obligations through intermediaries, enhancing the accountability of compliance systems.

6.4. Decentralized Autonomous Organizations (DAOs) and Corporate Compliance

The rise of DAOs—blockchain-based entities governed by decentralized decision-making—presents both transformative opportunities and significant challenges for corporate compliance. Unlike traditional firms, which rely on hierarchical governance, DAOs operate through smart contracts and token-based voting, automating many aspects of organizational management. While this structure enhances transparency and reduces opportunities for human-driven misconduct, it also complicates regulatory enforcement by dispersing accountability across a distributed network of token holders.

A key advantage of DAOs is their ability to embed compliance directly into algorithmic governance. By codifying regulatory requirements, such as anti-money laundering (AML) checks or conflict-of-interest policies, into smart contracts, DAOs can enforce rules programmatically, minimizing discretionary violations (De Filippi & Wright, 2020). For instance, a venture capital DAO could automatically reject transactions involving blacklisted wallet addresses or require multi-signature approvals for high-value transfers, ensuring adherence to sanctions regimes (Reijers *et al*., 2023). In another scenario, DAO managing supply-chain payments could auto-reject transactions lacking ESG certifications, aligning with “global anomie” harm-reduction principles. Furthermore, because all DAO decisions are immutably recorded on-chain, regulators and stakeholders gain real-time auditability, a significant improvement over the retrospective and often opaque compliance reviews of traditional corporations (Wright & De Filippi, 2022).

However, DAOs also introduce novel legal and regulatory challenges. Their decentralized nature makes it difficult to assign liability in cases of non-compliance, particularly in jurisdictions where DAOs lack legal personhood. Moreover, excessive reliance on smart contracts risks "algorithmic rigidity," where inflexible code fails to adapt to evolving regulatory requirements or unforeseen risks (Savelyev, 2017). These issues have led to ongoing debates over whether DAOs should be treated as legal entities or remain outside traditional corporate frameworks (Reijers *et al*., 2023).

To address these challenges, future regulatory approaches may need to adopt hybrid models that balance decentralization with accountability. One potential solution is the use of regulatory sandboxes, allowing DAOs to operate under supervised conditions while policymakers assess compliance risks in real time. Another approach involves integrating legal wrappers or human oversight committees into DAO structures, ensuring that algorithmic governance remains adaptable to legal standards without sacrificing the benefits of decentralization.

Ultimately, DAOs represent a fundamental shift in corporate governance, replacing centralized control with transparent, code-driven decision-making. While they offer powerful tools for automating compliance, their legal ambiguity and structural decentralization necessitate innovative regulatory frameworks. Policymakers must work alongside technologists and legal scholars to develop adaptive solutions that preserve the efficiency and transparency of DAOs while ensuring they operate within established legal and compliance boundaries. The success of these efforts will shape not only the future of blockchain-based organizations but also the broader evolution of corporate governance in an increasingly digital economy.

6.5. Cryptocurrency Transactions and Compliance Risks

The integration of cryptocurrency transactions into corporate finance introduces significant compliance challenges, particularly in areas such as AML and

Counter-Terrorist Financing (CTF). Unlike traditional banking transactions, cryptocurrency payments can be pseudonymous, making it more difficult to track illicit financial flows.

To address these risks, compliance programs have increasingly adopted blockchain analytics tools that trace cryptocurrency transactions across public ledgers (Foley *et al*., 2019). These tools use heuristics and machine learning algorithms to detect suspicious patterns, such as transaction structuring, mixing services, and wallet clustering, which are commonly associated with money laundering.

Additionally, regulatory agencies have mandated the use of blockchain-based identity verification systems, such as those leveraging zero-knowledge proofs (ZKPs) to balance user privacy with compliance obligations (Narayanan *et al*., 2022). These solutions enable compliance officers to verify transaction legitimacy without exposing sensitive personal data, enhancing both security and regulatory adherence.

Despite these advancements, significant regulatory gaps remain. Jurisdictions vary widely in their treatment of cryptocurrencies, with some enforcing strict AML/KYC requirements and others maintaining a more laissez-faire approach (Zohar, 2015). Compliance programs must navigate this fragmented regulatory landscape, ensuring that corporate cryptocurrency transactions remain compliant with evolving legal standards.

So, blockchain technology holds immense potential to transform corporate compliance beyond record-keeping. By enabling real-time monitoring, automating enforcement through smart contracts, integrating DAOs into compliance frameworks, and addressing the complexities of cryptocurrency transactions, blockchain-based compliance models can enhance transparency, reduce risks, and improve regulatory effectiveness. However, these innovations also introduce new legal and ethical challenges that require adaptive regulatory frameworks and continuous oversight.

7. CRIMINOLOGICAL PERSPECTIVES ON DIGITAL COMPLIANCE AND BLOCKCHAIN-BASED ENFORCEMENT

Perhaps we need to incorporate criminological theories to better understand and mitigate corporate deviance, financial crimes, and regulatory violations in digital and virtual environments: Passas' work on criminogenic asymmetries, global anomie, and the blurred boundaries between legal and illegal transnational activities offers a useful lens through which to analyze the risks posed by digital compliance models and blockchain-based enforcement mechanisms.

7.1. Criminogenic Asymmetries and Compliance Gaps in Virtual Environments

Regulatory loopholes in decentralized finance exemplify criminogenic asymmetries, allowing illicit financial flows to exploit jurisdictional gaps. Passas (1999) introduced the concept of criminogenic asymmetries, referring to structural imbalances in legal frameworks, regulatory enforcement, and economic opportunities that create conditions favorable for criminal activity. These asymmetries are particularly pronounced in digital environments where decentralized and borderless financial technologies, such as cryptocurrencies and DAOs, challenge traditional regulatory mechanisms (see also Dolliver and Love, 2021).

Blockchain-based compliance systems, while enhancing transparency and security, also create new asymmetries in regulatory oversight. For example, countries with weak financial regulations may become hubs for illicit crypto transactions, facilitating regulatory arbitrage where entities exploit jurisdictional differences to evade compliance (Passas, 1999, 2001, 2005). Similarly, DAOs, which lack traditional corporate hierarchies, present difficulties in assigning liability and ensuring accountability (Reijers *et al*., 2023).

To address these asymmetries, blockchain-based enforcement should incorporate compliance mechanisms that adapt to cross-border regulatory variations. Blockchain's permissioned ledgers can enforce jurisdiction-specific rules via smart contracts, reducing arbitrage opportunities (e.g., automatic tax withholding for cross-border transactions). One approach is the use of regulatory interoperability, where smart contracts and digital identity verification systems enforce jurisdiction-specific compliance obligations in real time (Zhao *et al*., 2022). Additionally, blockchain-based AML/KYC mechanisms can mitigate asymmetric risks by requiring firms to comply with the highest regulatory standards, reducing opportunities for arbitrage and non-compliance. Also, stablecoin issuers could embed real-time compliance checks into token protocols, preventing misuse in shadow banking, thereby addressing also "lawful but awful" practices.

So, blockchain can mitigate regulatory arbitrage through DAOs' ability to enforce jurisdiction-specific rules programmatically, while Metaverse simulations expose how asymmetries manifest in virtual economies.

7.2. Global Anomie and the Expansion of Compliance in Digital Economies

Passas (2000; see also Thiel, 2011; Twyman-Ghoshal, 2021) argued that economic liberalization, deregulation, and financialization have led to a state of global anomie—a breakdown of normative constraints in transnational economic activities. This condition fosters opportunities for illicit financial flows, regulatory evasion, and "lawful but awful" corporate behaviors that exploit legal loopholes.

Blockchain's decentralized structure challenges traditional enforcement models, reinforcing global anomie by creating compliance-free zones in digital economies. The proliferation of decentralized finance (DeFi) platforms and cryptocurrencies illustrates global anomie in action. These technologies enable financial transactions beyond the reach of traditional oversight, allowing bad actors to operate within legal gray areas while engaging in harmful practices (Campbell-Verduyn, 2018). For instance, DeFi lending protocols may comply with blockchain-based smart contract rules but simultaneously facilitate money laundering through privacy coins and mixer services.

A blockchain-based compliance model informed by global anomie theory would focus on harm reduction rather than purely law-based enforcement. This could involve proactive compliance analytics that detect patterns of systemic risk and unethical behavior before they escalate into full-scale financial crimes. Additionally, compliance mechanisms should be designed to respond dynamically to evolving risks, integrating AI-powered forensic tools to analyze transactions and detect emerging financial crime typologies (Fang *et al*., 2023). DAOs' decentralized governance models may challenge the "anomic" deregulation of digital economies by embedding compliance into their operational DNA, whereas Metaverse testing reveals how anomie develops in unmonitored virtual transactions.

7.3. The Legal-Illegal Interface and Regulatory Challenges of Digital Compliance

Passas (2003) has analyzed the legal-illegal interface, where legal economic activities intersect with illicit practices, creating opportunities for regulatory evasion and corporate misconduct. In digital finance, this interface is particularly evident in the rise of regulatory arbitrage, offshore cryptocurrency exchanges, and the use of blockchain-based anonymity tools.

One major challenge in digital compliance is distinguishing between lawful but awful corporate practices—activities that, while technically legal, exploit regulatory gaps for unethical purposes (Passas, 2005, 2016). Examples include:

- The use of stablecoins for shadow banking, bypassing traditional financial regulations.
- DAOs structuring themselves to avoid tax liabilities or corporate responsibility.
- The use of decentralized exchanges (DEXs) to facilitate tokenized insider trading.

Blockchain-based compliance mechanisms should be designed to detect and deter these practices by embedding ethical safeguards within decentralized financial ecosystems. This could involve algorithmic governance models that assess transactions for indicators of systemic harm, even if they do not violate specific legal statutes. For example, blockchain-based risk-scoring models could integrate ESG (Environmental, Social, and Governance) compliance indicators, ensuring that digital finance platforms prioritize ethical considerations alongside legal requirements (Zohar, 2015).

7.4. Criminogenic Risks in the Metaverse and Virtual Compliance Challenges

As corporations expand their operations into the Metaverse, new forms of digital deviance emerge, including virtual fraud, metaverse-based money laundering, and regulatory evasion through digital assets. Passas' criminogenic asymmetries framework suggests that virtual regulatory gaps will enable actors to exploit digital environments for financial crime.

For instance, Metaverse economies introduce unregulated financial ecosystems where assets such as NFTs (non-fungible tokens) and virtual currencies can be used for money laundering, tax evasion, and illicit market manipulation (Davidson *et al*., 2018). Compliance programs must therefore extend beyond traditional financial regulations to address the criminogenic risks of virtual environments.

One potential solution is the integration of blockchain-based digital identity verification systems into Metaverse platforms, ensuring that transactions are traceable and compliant with AML regulations (Casino *et al*., 2019). Additionally, compliance programs could incorporate AI-driven behavioral monitoring tools to detect suspicious activity within virtual spaces, such as coordinated market manipulation in virtual real estate markets or wash trading of NFTs (Wright & De Filippi, 2022).

This criminological perspective on blockchain-based compliance highlights the need for regulatory frameworks that account for global asymmetries, anomic financial behaviors, and the legal-illegal interface in digital economies. By integrating criminogenic risk assessment into digital compliance mechanisms, blockchain-based enforcement can move beyond punitive measures toward proactive harm reduction. However, these strategies require cross-border regulatory cooperation and continuous adaptation to evolving technological and criminogenic threats.

8. UTILIZING THE METAVERSE TO TEST THE EFFECTIVENESS OF COMPLIANCE PROGRAMS

While acknowledging the concerns raised in the academic literature regarding digital compliance, our proposal aims to address these criticisms by structuring an interaction model with AI tools that enhances the predictability and reliability of effectiveness testing for compliance programs.

To achieve this objective, we propose leveraging the simulation capabilities of the Metaverse (Pantaleo, 2024). By creating a digital twin of a corporate environment within a virtual ecosystem, the Metaverse could enable real-time, controlled testing of specific compliance programs, allowing for an empirical assessment of their preventive efficacy (Coppola, 2022).

The possibility of testing human activities in the Metaverse before carrying them out in the real world has already been explored in the medical field, where virtual environments have been used to assess the effects of certain therapies prior to their actual adoption (Kawarase & Anjankar, 2022).

Similarly, in the educational domain, students have had the opportunity to practice courtroom hearings in a MetaCourt, allowing them to develop the necessary skills for their future profession as lawyers (De Vita, 2023).

Turning to the corporate world, we argue that visually replicating the functioning of compliance protocols and subjecting them to stress tests designed to assess their resilience against corporate crime risks could address some of the primary concerns associated with invasive employee monitoring. In this framework, what is being observed and evaluated are not individual employees in their physical capacity but rather their digital avatars, which serve as proxies for corporate roles rather than real persons. This distinction could significantly mitigate ethical and legal concerns regarding workplace surveillance while still allowing companies to test and refine their compliance mechanisms in a risk-free, simulated environment.

Moreover, subjecting corporations to testing within the Metaverse could yield significant benefits regardless of the outcome of the assessment.

If the test produces a positive result, the corporation would gain reassurance regarding the validity of its preventive measures. However, even in this scenario, the corporation would need to rigorously implement the validated model, participate in periodic updates of the testing framework, and ensure continuous engagement with the necessary information flow.

Conversely, in the event of a negative result, the organization could adapt its compliance model to align with emerging standards identified through the simulation.

To certify the results and the frequency of the tests conducted, blockchain technology could be employed. Given its ability to securely record specific data—such as test outcomes and their recurrence—while ensuring probative reliability due to the extreme difficulty, if not impossibility, of fraudulent alterations, each time a corporation undergoes simulation in the Metaverse, its outcome should be recorded via blockchain. This record could then be used as evidence in criminal proceedings.

Before delving into the details of how the proposed interaction model between artificial intelligence and corporate criminal compliance operates, two further clarifications are necessary.

The first concerns the credibility of the test: for the assessment to be considered reliable, it must be conducted on a case-by-case basis, taking into account the specific characteristics of each individual corporation under evaluation. Otherwise, the test risks being deemed too generic and, consequently,

ineffective in addressing the unique features and compliance challenges of the organization in question.

The second clarification concerns the legal authority over the final assessment: despite the Metaverse simulation, the ultimate decision regarding the effectiveness of the compliance model would remain within the jurisdiction of the judicial authority. Nonetheless, a positive test outcome should require a heightened standard of reasoning in cases where the judicial authority seeks to deem the compliance program ineffective despite the favorable test result and its subsequent updates.

Having defined the framework within which the simulation operates, we can now assess the potential of Metaverse-based compliance.

The digital suitability test of the compliance model first requires the Metaverse to accurately replicate the functioning of the preventive measures adopted by the corporations under evaluation. Naturally, this entails the creation of a digital replica at the avatar scale—that is, a virtual representation of the company's decision-making and behavioral processes, as outlined in its adopted preventive protocols.

This process would thus generate a corporate prototype in which the preventive mechanisms are precisely reproduced—even visually—within the Metaverse, allowing for an interactive and dynamic assessment of their effectiveness.

As one might expect, the broader the participation of corporations in the policy-building phase within the Metaverse and the more they share their compliance programs, the greater the opportunity for comparative evaluation of the measures adopted. Furthermore, leveraging AI capabilities would facilitate the identification and clustering of best practices across different corporate groups, thereby enhancing the overall effectiveness of compliance strategies.

The second step of the Metaverse simulation involves the actual testing of the preventive measures against corporate crime risks. In other words, the corporate clone operating within the Metaverse must now be exposed to the potential threats arising from corporate crimes.

To achieve this, it is essential to identify real-world scenarios in which the risk of criminal conduct could materialize and translate them into digitalized simulations within the Metaverse. This process allows for an empirical assessment of how effectively the compliance measures can mitigate such risks in a controlled virtual environment.

This is arguably the most complex data collection operation. However, with certain necessary approximations, it can be accomplished.

After all, compliance programs require not the absolute elimination of any risk related to predicate offences but rather their reasonable and continuous reduction.

Once the company's preventive efforts are defined in these terms, the collection of risk-related data can draw from a range of qualified sources—foremost among them, judicial practice.

Through court rulings on corporate liability for criminal offences, it is possible to codify the risk scenarios that companies have encountered and assess the effectiveness (or shortcomings) of the preventive protocols they have adopted. This body of knowledge should be further enriched through a multi-stakeholder public-private collaboration, involving trade associations, academia, the judiciary, and legal professionals to identify concrete risks that corporations must mitigate. Additionally, where available, well-established best practices should be integrated into the dataset to enable a comparative analysis with the measures actually implemented by the corporation.

Among all stakeholders, we believe that the success of the simulation critically depends on the participation of judicial representatives, particularly those specializing in corporate criminal liability.

Without the contribution of prosecutors and judges in defining the relevant risks and the essential preventive protocols to be adopted, any form of testing would risk being dismissed as overly abstract and disconnected from practical experience. Moreover, involving judicial authorities in shaping the content of the Metaverse simulation could foster their willingness to recognize the validity of the test results. This, in turn, could contribute to the development of a more consistent and uniform judicial approach to corporate compliance.

As previously outlined, the comparison between the compliance program reproduced in the Metaverse and the risks and best practices identified by stakeholders leads to the final step of the test: assessing the

resilience of corporate preventive measures in effectively countering foreseeable corporate crime risks.

The evaluation process is initially conventional in nature. However, thanks to advanced data collection capabilities, it can progressively evolve into an increasingly automated procedure—while, in our view, consistently respecting the human-in-control principle. At the outset, Artificial Intelligence—understood here as the Metaverse—should be tasked exclusively with virtually replicating both the compliance program of the corporation undergoing the test and the situational risks of corporate crime, as identified through judicial data and by relevant stakeholders for the specific type of entity involved.

In this way, the AI system will be able to detect potential gaps in the compliance program with respect to the situational risks under consideration. More precisely, it will highlight such gaps by directly comparing the preventive measures actually adopted with the crime-related risks identified. The system will assess whether the entity has implemented all necessary safeguards to address the full spectrum of risks arising from situational factors, as documented in judicial cases. By interacting with the simulation, stakeholders may further identify additional weaknesses or propose improvements to the corporation's compliance structure aimed at preventing corporate crimes.

As the AI system incorporates feedback provided by human stakeholders during the simulations, the evaluation process may become increasingly automated, gradually developing the capacity to autonomously recognize both preventive gaps and appropriate corrective measures, in line with patterns and recommendations historically identified by expert users.

That said, as previously emphasized, the final judgment regarding the outcomes generated by the system must remain in the hands of the human stakeholders involved in the simulation. In this sense, the Metaverse emerges as an advanced instrument for conducting dynamic, expert-driven compliance testing.

Finally, it should be stressed that the simulation is not intended to replace judicial evaluation of the efforts made by corporations to prevent corporate crimes. Rather, its purpose is to serve as a supporting tool—one that can assist such evaluations and enhance their predictability from the perspective of the corporation.

9. TEST OUTCOMES

The test outcome could take one of three forms:

1. **Green Flag**: The test confirms that the company has adopted preventive measures addressing all identified risks and that its policies fully align with those recognized by experts as reliable for the specific risk category.

2. **Yellow Flag**: The test reveals that while the company has accounted for all digitized risks, some of its adopted measures do not fully correspond to best practices. In this scenario, allowing experts to access the virtual simulation and its results could introduce a valuable dialogical dimension. Experts could integrate Metaverse-generated data almost in real-time, providing targeted recommendations on which policies should be adjusted or replaced with more effective alternatives.

3. **Red Flag**: The simulation exposes significant deficiencies in both the identification of relevant risks and the selection of preventive measures adopted to mitigate them.

In cases where deficiencies are identified, the company should adjust its preventive policies until they achieve full compliance. The greater the volume of data gathered through corporate participation in Metaverse-based compliance testing, the more precise and data-driven the preventive restructuring process will be.

All test results should then be secured and certified via blockchain to ensure their integrity and probative value. Moreover, the test should be repeated periodically, particularly when the compliance model undergoes updates or when new risks emerge. This test is operationalized in Box **1**.

10. THE METAVERSE AND DIGITAL COMPLIANCE TESTING: OPPORTUNITIES AND RISKS

Current digital compliance testing methods primarily rely on automated auditing tools, algorithmic risk assessments, and AI-driven transaction monitoring systems. These technologies analyze structured financial and operational data to detect regulatory breaches, offering consistency and efficiency in compliance verification. Blockchain-based compliance mechanisms, for instance, rely on immutable ledgers and smart contracts to enforce rules and provide tamper-proof audit trails (Casino *et al*., 2019).

To translate the diagnostic potential of Metaverse-based compliance testing into tangible organizational improvements, a structured approach is essential. We propose a three-tiered classification system, defined by explicit thresholds and accompanied by clear implementation criteria. This framework ensures that the insights gleaned from virtual simulations directly inform and drive enhancements within compliance programs.

1. Green Flag: Demonstrating Comprehensive Compliance Alignment

A "Green Flag" outcome signifies that an organization's proactive measures effectively mitigate identified risks, with established policies meeting or exceeding recognized best practices. Achieving this classification requires adherence to the following rigorous thresholds:

- **Risk Coverage:** A minimum of 95% of digitized risk scenarios (encompassing areas such as bribery, money laundering, and data breaches) must be addressed by documented protocols. Any residual gaps must be demonstrably limited to low-impact risks, constituting less than 5% exposure as defined by ISO 31000.
- **Policy Adherence:** The organization's protocols must align with 95% or more of the benchmarks established by authoritative frameworks relevant to their operations (e.g., U.S. Sentencing Guidelines, ISO 37301, or FATF standards for AML). Furthermore, evidence of continuous improvement, such as annual policy updates reflecting evolving regulatory landscapes, is a prerequisite.
- **Validation:** The effectiveness of these measures must be independently verified through a minimum of three simulated stress tests per risk category, conducted by independent auditors or AI-driven tools. All test results must be immutably recorded on a blockchain platform (e.g., Hyperledger Fabric) to ensure data integrity and auditability.

Organizational Actions Following a Green Flag:

- The organization will be granted a blockchain-secured compliance certificate, valid for a period of 12 months and renewable upon successful retesting.
- A summary of the positive test outcomes will be disclosed in the organization's ESG reports, thereby enhancing transparency for stakeholders.

2. Yellow Flag: Addressing Partial Compliance Gaps

A "Yellow Flag" indicates that while all material risks have been identified by the organization, the controls in place for one or more high-impact risk categories exhibit suboptimal efficacy. The thresholds for this classification include:

- **Risk Identification:** All digitized risks must be cataloged within the organization's framework. However, at least one control mechanism must fail to meet established efficacy thresholds (e.g., demonstrating a detection rate of less than 70% for fraudulent activities in simulations).
- **Policy Shortfalls:** The identified control deficiencies must stem from deviations from best practices in no more than two of the following critical areas:
    - **Timeliness:** Instances where manual processes are employed despite industry standards favoring automation.
    - **Coverage:** Situations where the scope of controls is insufficient (e.g., regional AML checks lacking integration across international operations).
    - **Enforcement:** Evidence of inconsistent application of disciplinary measures for policy violations.
- **Expert Intervention:** Upon a "Yellow Flag" outcome, compliance specialists must conduct real-time reviews, providing the organization with:
    - A prioritized remediation roadmap outlining specific actions and timelines (e.g., "Implement AI-driven anomaly detection for expense reports within 90 days").
    - Benchmarked alternatives, suggesting peer-approved and effective solutions (e.g., "Adopt peer-approved smart contracts for procurement processes").

Organizational Actions Following a Yellow Flag:

- Critical compliance gaps must be fully addressed within a 60-day timeframe, while moderate gaps require remediation within 180 days. Progress on these milestones will be diligently tracked via blockchain records.
- Monthly Metaverse retests will be mandatory for the specific risk categories where deficiencies were identified until a "Green Flag" status is achieved.

3. Red Flag: Rectifying Systemic Compliance Failures

A "Red Flag" signifies a critical situation characterized by either a failure to identify material risks or the presence of systemic breakdowns within the organization's control environment. The thresholds for this severe classification include:

- **Risk Blind Spots:** The organization has failed to address at least one risk from a mandatory list of critical exposures (e.g., corruption in high-risk markets) or demonstrates a deviation of more than 40% from established sector benchmarks (e.g., NIST standards for cybersecurity).
- **Control Failures:** Simulations conducted within the Metaverse environment reveal significant deficiencies, including:
    - 50% or more of policy violations going undetected by existing controls.
    - 40% or more of detected violations not resulting in appropriate corrective actions.
- **Root Causes:** Blockchain logs generated during testing must pinpoint recurrent underlying flaws within the compliance framework (e.g., "35% of simulated onboarding transactions bypassed mandatory KYC checks").

Organizational Actions Following a Red Flag:

- High-risk operational activities (e.g., cross-border payments, handling of sensitive data) must be immediately paused until effective interim controls are implemented and verified.

- A comprehensive redesign of the organization's compliance programs is required, involving external consultants to ensure objectivity and expertise. The revised programs must undergo iterative validation through rigorous Metaverse testing.
- All new or significantly revised policies must receive explicit board-level approval. Furthermore, the organization must provide quarterly progress reports on remediation efforts to relevant regulatory bodies.
- The persistence of identified gaps beyond a 90-day remediation period will trigger the issuance of a Material Weakness Report, in accordance with regulations such as SOX or Legislative Decree 231/2001.

Implementation Framework: Embedding the Tiered System

To effectively institutionalize this three-tiered classification system and ensure its ongoing utility, organizations should adopt the following implementation framework:

- **Conduct Annual and Trigger-Based Testing:** Full-scope Metaverse simulations should be conducted on an annual basis. Additionally, trigger-based retests should be initiated within 30 days of any significant regulatory changes or internal compliance incidents.
- **Leverage Blockchain for Immutable Records:** Permissioned blockchain ledgers (e.g., Quorum) should be utilized to immutably record all critical data related to testing, including test parameters, simulation results, and commitments to remediation actions. This ensures transparency and facilitates robust auditing.
- **Automate Escalation and Notification:** Integrated dashboards (e.g., leveraging Power BI and Ethereum smart contracts) should be implemented to automate the escalation process. "Yellow Flag" outcomes will trigger immediate alerts to relevant compliance officers, while "Red Flag" outcomes will automatically notify regulatory authorities and the organization's audit committee, prompting immediate governance reviews.

Example Application:

Consider a financial institution that receives a "Yellow Flag" following Metaverse-based AML testing. The simulations reveal that 30% of simulated cryptocurrency transactions evade existing detection mechanisms. In response, the institution is required to integrate blockchain analytics tools (e.g., Chainalysis) within 60 days to enhance their monitoring capabilities. Subsequently, they must undergo retesting in the Metaverse environment to demonstrate improved detection rates and achieve "Green Flag" status.

By systematically embedding these clearly defined thresholds and implementation criteria, the Metaverse-based compliance testing model transcends its theoretical potential, evolving into a scalable and auditable tool that directly supports real-world governance demands and drives continuous improvement in organizational compliance.

Box 1: Operationalizing Compliance Test Outcomes: A Tiered Framework for Actionable Insights.

By contrast, the Metaverse introduces a more dynamic, behavior-oriented environment for compliance testing. Rather than depending solely on static data analysis, it enables real-time simulations in which corporate actors engage in virtual decision-making. This allows compliance officers to evaluate ethical reasoning, procedural adherence, and the robustness of fraud detection protocols within simulated real-world scenarios. Such an interactive model complements traditional tools by offering behavioral insights that conventional data analysis may overlook.

For example, companies may employ the Metaverse to stress-test compliance programs by simulating corruption schemes, cybersecurity breaches, or financial fraud within immersive corporate environments. These simulations enable organizations to refine internal policies and training procedures in ways that go beyond the capacities of conventional analytics (Davidson *et al*., 2022).

A key advantage of Metaverse-based compliance lies in its capacity—once an adequate dataset is established—to allow organizations to benchmark their preventive efforts against those of peer entities and expert standards, all within a short time frame and through an intuitive visual interface. The graphical reproduction of compliance protocols further enhances employee training, enabling staff to observe best practices in action within a simulated space.

Moreover, conducting compliance evaluations in virtual reality may help circumvent data privacy and surveillance concerns—particularly under the GDPR. Since the Metaverse simulates depersonalized employee avatars, individual behaviors are not subject to scrutiny. Instead, the focus shifts to abstract, anonymized behavioral models, ensuring personal data protection while maintaining rigorous compliance testing.

Despite its potential, several technical constraints may limit the reliability and scalability of Metaverse-based compliance tools:

- Complexity of Real-World Replication: While Metaverse environments can simulate compliance dynamics, they struggle to replicate the full complexity of human decision-making and adaptive criminal behaviors. Unlike financial compliance algorithms that process large-scale structured data, virtual simulations are bound by predefined programming, which may fail to anticipate novel or context-specific challenges (Zhao *et al*., 2022).

- Data Integrity and Verification: The reliability of simulated outputs depends heavily on the quality of input data and decision-making models. Simulations based on incomplete or biased data may foster a false sense of security about the effectiveness of compliance protocols. Unlike blockchain systems, which offer immutable records, Metaverse-generated insights can be misinterpreted or manipulated.

- Scalability Constraints: While feasible for certain corporations, large-scale deployment across jurisdictions remains problematic. Traditional AI-powered compliance tools already operate at a global scale, detecting cross-border financial crimes in real time. By contrast, Metaverse-based testing lacks standardized frameworks, limiting its applicability to multinational corporations.

One of the most evident practical challenges lies in the complexity and cost of gathering and processing the data needed for such simulations. However, this should not discourage innovation. Notably, a recent U.S. criminal trial employed the Metaverse to allow a judge to reconstruct the sequence of events from the defendant's perspective, assessing the applicability of the "Stand Your Ground" law.

As the Metaverse becomes increasingly embedded in professional and everyday life, accessibility will likely improve—driven by market competition and technological advances. This evolution will naturally reduce the investment threshold for developing simulations like the one envisioned here. In the interim, organizations may begin collecting the foundational data needed for future implementation.

At the same time, integrating the Metaverse into compliance testing introduces novel regulatory and operational risks, particularly regarding identity verification, financial transactions, and cross-jurisdictional enforcement:

- Identity Fraud and Anonymity: The use of avatars complicates identity verification and accountability. Malicious actors could exploit anonymity to impersonate personnel or circumvent digital oversight mechanisms (Wright & De Filippi, 2022).

- Virtual Financial Crimes: The presence of digital assets, NFTs, and cryptocurrencies in Metaverse economies raises concerns about unregulated transactions and potential laundering schemes. In contrast to traditional financial institutions, many Metaverse platforms fall outside formal AML and KYC regimes (Fang *et al*., 2023).

- Regulatory Fragmentation: The transnational nature of the Metaverse poses significant enforcement challenges. Companies conducting compliance operations in virtual settings must navigate fragmented legal frameworks, increasing exposure to legal uncertainty and liability (Reijers *et al*., 2023).

In conclusion, the Metaverse offers significant potential to revolutionize compliance testing by enabling real-time, behavior-focused simulations that complement traditional digital tools. Nevertheless, its efficacy is tempered by current limitations—technical, regulatory, and procedural. To fully harness its capabilities, regulatory bodies must establish standardized frameworks that not only address these emerging risks but also promote the responsible use of immersive technologies in corporate compliance.

REFERENCES

Burchard, C. 2020. The "Criminal Law" of predictive society… or how "smart" algorithms (could) change the administration of criminal justice. Law and Order (1): 1-5.

Campbell-Verduyn, M. 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change 69(2): 283-305. https://doi.org/10.1007/s10611-017-9756-5

Casino F., Dasaklis T. K., & Patsakis C. 2019. A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telematics and Informatics 36: 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Cong L. W., & He Z. 2019. Blockchain disruption and smart contracts. The Review of Financial Studies 32(5): 1754-1797. https://doi.org/10.1093/rfs/hhz007

Coffee, J. C. Jr. 1990. "Carrot and Stick" Sentencing: Structuring Incentives for Organizational Defendants. Fed. Sent. Rep. (3): 126-129. https://doi.org/10.2307/20639307

Coppola, F. 2022. "Digital Compliance and Crime-Prevention: How AI and Metaverse May Improve the Effectiveness of Compliance Programs". Iura and Legal Systems (4): 98-102.

Davidson S., De Filippi P., & Potts J. 2018. "Blockchains and the economic institutions of capitalism". Journal of Institutional Economics 14(4): 639-658. https://doi.org/10.1017/S1744137417000200

Davidson S., De Filippi P., & Potts J. 2022. "The economics of NFTs and the regulatory challenges of virtual assets". Journal of Financial Regulation 8(1): 77-102.

De Filippi P., & Wright A. 2020. Blockchain and the law: The rule of code: Harvard University Press.

De Vita, V. 2023. "Salerno, processo MetaCourt: la prima simulazione di un dibattimento penale all'Università", Il Mattino, November 29, p.1.

Dolliver D., & Love K. 2015. "Criminogenic Asymmetries in Cyberspace: A Comparative Analysis of Two Tor Marketplaces". Journal of Globalization Studies 5(2): 75–96.

Fang F., Liu M., & Wong W. K. 2023. "Anti-money laundering in the age of cryptocurrencies: A review of blockchain-based compliance solutions". Journal of Financial Crime 30(1): 102-118.

Fiorella A. 2016. "Dogmatica e responsabilità ex crimine delle persone giuridiche". Riv. Trim. Dir. Pen. Econ. 3-4: 633-649.

Foley S., Karlsen J. R., & Putniņš T. J. 2019. "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" The Review of Financial Studies 32(5):1798-1853. https://doi.org/10.1093/rfs/hhz015

Forti G. 2012. "Uno sguardo ai "piani nobili" del d.lgs. n. 231/2001". Riv. It. Dir. Proc. Pen. 2:1249-1298.

Gargani A. 2002. "Imputazione del reato agli enti collettivi e responsabilità penale dell'intraneo: due piani irrelati?". Diritto penale e processo 9: 1061-1069.

Gullo A. 2023. Compliance. Archivio penale 1: 1-17.

Manes V. 2021. "Realismo e concretezza nell'accertamento dell'idoneità del modello". Giurisprudenza commerciale 4: 633-661.

Mongillo V. 2011. "Il giudizio di idoenità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione". La responsabilità amministrativa delle società e degli enti 3: 69-100.

Mongillo V. 2023. "La colpa di organizzazione: enigma ed essenza della responsabilità "da reato" dell'ente collettivo". Cassazione penale 3: 704-736.

Mongillo V. 2022. "Presente e future della compliance penale". Sistema penale: 1-21.

Morgente G., & Fiorinelli G. 2022. "Promesse e rischi della compliance penale digitalizzata". Archivio penale 2: 1-41.

Narayanan A., Bonneau J., Felten E., Miller A., & Goldfeder S. 2022. Bitcoin and cryptocurrency technologies: Princeton University Press.

Nisco A. 2022. "Riflessi della compliance digitale in ambito 231". Sistema penale: 1-12.

Kawarase M. A. 4th, & Anjankar A. 2022. "Dynamics of Metaverse and Medicine: A Review Article". Cureus 14 (11): 1-6. https://doi.org/10.7759/cureus.31232

Paliero C. E., & Piergallini C. 2006. "La colpa di organizzazione". Responsabilità amministrativa società enti 3: 167-184.

Pantaleo D. 2024. Metaverso e diritto penale: Pacini Giuridica.

Passas N. 1999. "Globalization, criminogenic asymmetries and economic crime". European Journal of Law Reform 1(4): 399-423.

Passas N. 2000. "Global anomie, dysnomie, and economic crime: Hidden consequences of neoliberalism and globalization in Russia and around the world". Social Justice 27(2): 16-44.

Passas N. 2003. "Cross-border crime and the interface between legal and illegal actors". Security Journal 16(1): 19-37. https://doi.org/10.1057/palgrave.sj.8340123

Passas N. 2005. "Global Anomie Theory and Crime". Pp. 174-182 In The Essential Criminology Reader edited by S. Henry & M. Lanier. Boulder, CO: Westview Press. https://doi.org/10.4324/9780429496592-22

Passas N. 2005. "Lawful but awful: 'Legal Corporate Crimes'". The Journal of Socio-Economics 34(6): 771-786. https://doi.org/10.1016/j.socec.2005.07.024

Passas N. 2016. "Legal Crimes - Lawful but Awful". Pp. 125-127 in A Companion to Crime, Harm and Victimisation edited by K. Corteen, S. Morley, P. Taylor, & J. Turner. Bristol: Policy Press.

Reijers W., O'Dwyer R., & Bodo B. 2023. "The governance of blockchain-based organizations: A socio-legal perspective". New Media & Society 25(2): 342-361.

Savelyev A. 2017. "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law". Information & Communications Technology Law 27(1): 85-123. https://doi.org/10.1080/13600834.2017.1301036

Thiel S. 2011. "Global Anomie and India: A Conceptual Approach". Indian Journal of Asian Affairs 24(1/2): 17-34.

Twyman-Ghoshal A. 2021. "Global Anomie Theory". In Oxford Research Encyclopedia of Criminology and Criminal Justice: Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.545

Wright A., & De Filippi P. 2015. "Decentralized blockchain technology and the rise of lex cryptographia". SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2580664

Wright A., & De Filippi P. 2022. "Decentralized blockchain-based organizations and the law". Computer Law & Security Review 38: 105655.

Zhao, Y., Chen, L., & Xu, X. 2022. "The impact of blockchain on regulatory compliance: Challenges and opportunities". Journal of Business Ethics 179(3): 593-614.

Zohar A. 2015. "Bitcoin: under the hood". Communications of the ACM 58(9): 104-113. https://doi.org/10.1145/2701411

Received on 24-02-2025 Accepted on 22-03-2025 Published on 25-04-2025

https://doi.org/10.6000/1929-4409.2025.14.09