Indonesian Journal of Multidisciplinary Sciences (IJoMS)
Vol. 5 No. 1 2026, 1235-1241
E-ISSN: 2963-7635 | P-ISSN: 2986-2426
Publisher: CV. Era Digital Nusantara

Targeting Intangible Entities: Mechanisms for Enforcing Cross-Border Data Crimes in Decentralized Autonomous Organizations (DAOs)

Jeisika Laurens, Yasmirah Mandasari Saragih, Alnur Syafrizul Arif, Azikri Hidayat Tulloh, Jackson Andre William, Muhammad Alvian Putera
Universitas 17 Agustus 1945 Jakarta
Corresponding email: jeisikalaurens01@gmail.com

ARTICLE INFO

Article History
Submission : 08-06-2026
Received : 09-06-2026
Revised : 22-06-2026
Accepted : 25-06-2026

Keywords
DAO;
Cyber Law Enforcement;
the Personal Data Protection Act
Government Regulation in Lieu of Law No. 1 of 2024;
Proxy Liability

DOI:
10.59066/ijoms.v5i1.2535

ABSTRACT

Decentralized Autonomous Organizations (DAOs), which operate through smart contracts without a legal entity, pose a fundamental challenge to cross-border data protection regimes. Following the enactment of Government Regulation in Lieu of Law No. 1 of 2024 amending the Personal Data Protection Act, enforcement mechanisms in Indonesia still rely on identifying "Personal Data Controllers" in the form of corporate or natural persons. When the flow of Indonesian citizens' data becomes the subject of criminal acts by a DAO into a non-equivalent jurisdiction, an absolute liability gap arises because there is no legal entity that can be sanctioned. This normative legal research employs a legislative, conceptual (cyber jurisdiction), and comparative approach, drawing on the legal frameworks of the European Union (GDPR) and Wyoming (DUNA). The study finds that conventional mechanisms suffer from structural failures. To address this issue, the study proposes a hybrid law enforcement mechanism: first, the application of proxy liability to key actors (core developers) as de facto data controllers; second, a regulatory mandate for a "legal wrapper" under the implementing regulations of the Personal Data Protection Act, requiring DAOs to have a legal representative in Indonesia as a prerequisite for cross-border data transfers, with on-chain access blocking via ISPs serving as a last resort.

Introduction

Advances in Web3 and blockchain technology have given rise to a new paradigm of business organization known as the Decentralized Autonomous Organization (DAO). Unlike conventional corporations, DAOs operate entirely through computer code (smart contracts) without a board of directors, a physical headquarters, or legal entity status. Decisions are made anonymously by token holders from various countries.

On the other hand, Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law), which was subsequently amended via Government Regulation in

Lieu of Law (Perppu) No. 1 of 2024. With the introduction of the new National Criminal Code, the term "violation" has been progressively replaced by the concept of "criminal offense," which carries stricter penalties. However, in both the PPDL and criminal law, law enforcement always requires the existence of a legal subject in the form of a natural person (natuurlijke persoon) or a legal entity (rechtspersoon).

Problems arise when a DAO, which lacks legal entity status, processes data—potentially leading to cross-border leaks of Indonesian citizens' personal data. Law enforcement authorities face an absolute liability gap, as there is no entity that can be identified as a "Personal Data Controller." Conventional law is unable to reach decentralized architectures. Therefore, a breakthrough in law enforcement mechanisms is needed to hold this intangible entity accountable.

Method

This study employs a normative legal research method (doctrinal legal research), which involves examining written legal materials through library-based research. This approach was chosen because the study aims to formulate new legal policies (specifically, the concepts of proxy liability and legal wrapper) to address legal loopholes resulting from the development of DAO technology.

Results and Discussion

Proxy Liability Mechanism for Key Actors (Core Developers) in DAOs

Indonesian positive law, particularly in the context of Government Regulation in Lieu of Law (Perppu) Number 1 of 2024, recognizes a layered system of criminal liability. Criminal sanctions may be imposed on corporations as well as on leaders or administrators who commit, order, or participate in criminal acts. However, DAOs fall outside this logic because they lack articles of incorporation, tax identification numbers, or a board of directors. When the personal data of Indonesian citizens is leaked into foreign jurisdictions through DAO smart contracts, a legal deadlock arises. To address this deadlock, it is necessary to determine how the data security architecture is designed, where the data flows, and how private keys are stored.

According to Saragih, in the context of criminal liability, a person may be held accountable if the element of fault (schuld) is fulfilled, whether in the form of intent or negligence. If a Core Developer designs a smart contract that by default weakens data protection (for example, by failing to encrypt personal data during cross-border transfers), then the element of fault is present. Such a developer cannot hide behind the argument of "decentralization," because in factual terms he or she is the "brain" behind the system that causes harm. This analogy is consistent with the principles governing corporate crime, where senior executives or management who issue instructions or fail to exercise proper supervision may be held personally liable in addition to the corporation itself. Therefore, the Personal Data Protection Supervisory Authority may designate the Core Developer as the

party exercising ultimate control over data processing, making the developer personally criminally liable if the architecture he or she built results in cross-border data breaches.

Operational Mechanisms of Law Enforcement through On-Chain Forensics

The application of Proxy Liability does not mean that law enforcement simply waits passively for perpetrators to surrender. Because DAOs operate anonymously, law enforcement mechanisms must be adapted to the underlying technology. Enforcement against cybercrime requires a specialized approach that uses information technology both as evidence and as a tracing tool. This is achieved through blockchain transaction tracing, commonly referred to as on-chain forensics.

When a data-related offense occurs, cybercrime units within the Indonesian National Police coordinate with the Personal Data Protection Supervisory Authority to trace the smart contract address responsible for the data leakage. From this address, investigators can track the flow of funds (cryptocurrency) received by the Core Developer as compensation for writing the code. This approach forms part of a criminological strategy for addressing cybercrime, in which digital footprints are used to implement the Proxy Liability mechanism. This does not mean prosecuting the DAO itself, but rather prosecuting the human actors behind the system as de facto Personal Data Controllers.

Classification of Core Developers as De Facto Data Controllers and Criminal Law Subjects

In Indonesian criminal law theory, criminal liability is attached to legal subjects. Traditionally, criminal law subjects consist of natural persons (natuurlijke persoon) and legal entities (rechtspersoon). A DAO, as a virtual entity, does not meet the criteria of a legal entity as regulated under the Commercial Code or company law. As a result, a gap emerges between technological reality and legal constructs. However, in the development of modern criminal law, particularly in the context of information technology crimes, the focus of liability may shift to parties exercising factual control (de facto controllers).

Legally, DAOs are claimed to operate automatically, but technically, smart contracts do not emerge on their own. There are humans who write the code, define the data-processing logic, and deploy the code onto the blockchain network. These actors are known as Core Developers. From the perspective of Proxy Liability, a Core Developer may be qualified as a perpetrator because he or she exercises control that enables the identification of those responsible. The investigation continues until the funds are converted into Indonesian Rupiah through a crypto exchange that is registered and verified by the Indonesian commodities authority (Bappebti).

At this stage, anonymity disappears, because crypto exchanges are required to implement Know Your Customer (KYC) procedures. The Core Developer's official identity—national ID, tax number, and bank account—will be revealed and can immediately become the object of arrest and criminal investigation under the Personal Data Protection Law. This approach gains strong legitimacy when viewed through comparative studies of European Union jurisdictions. Under the GDPR regime, European data protection authorities

have on several occasions successfully imposed fines and criminal sanctions on individual programmers who developed malicious decentralized applications, on the grounds that code creators cannot evade legal responsibility for the harmful consequences of their products on citizens' privacy rights. This demonstrates that the criminal justice system must be capable of adapting to new modes of crime that employ advanced technology.

The Regulatory Mandate for Legal Wrappers as a Means to Close Liability Gaps

The Proxy Liability mechanism discussed above has a fundamental limitation: it is reactive in nature (waiting for a data breach to occur) and heavily dependent on the technical expertise of law enforcement in digital tracing. If a Core Developer uses crypto mixers (tools designed to obfuscate digital transaction trails) or resides in a country without an extradition treaty with Indonesia, enforcement efforts may fail entirely. Therefore, a long-term, preventive, and structural mechanism is required—namely, mandating DAOs to adopt a Legal Wrapper.

Concept and Policy Formulation of Legal Wrappers in Indonesia

A Legal Wrapper is a legal instrument that requires an otherwise formless entity (such as a DAO) to wrap itself within a state-recognized legal entity. The purpose is not to alter the technological nature of DAOs, but to provide a legal "nameplate" that the law can strike in the event of a dispute. From the perspective of criminal law policy (penal policy), this constitutes a form of penal reform aimed at anticipating crime in the era of digital globalization.

The proposed policy formulation for Indonesia is to issue a Government Regulation as an implementing regulation of the Personal Data Protection Law. Such regulation should include a mandatory provision stating: "Any DAO-based entity that collects, processes, or serves as a destination for the transfer of personal data of Indonesian citizens from foreign jurisdictions must have a Legal Representative in the form of an Indonesian legal entity (e.g., a limited liability company or partnership)."

This legal representative functions as a "bridge." The DAO does not need to maintain a physical office, but it must designate a legal entity in Indonesia whose name is listed in the DAO application's privacy policy. This entity is considered de jure (legally) as the Data Controller. If, at a later stage, a data breach offense occurs through a DAO smart contract, the Personal Data Protection Supervisory Authority no longer needs to search for anonymous Core Developers abroad. The party that can be directly sued, fined, and have its assets seized is the DAO's legal representative in Indonesia. This policy aligns with broader efforts to protect victims of cybercrime, ensuring legal certainty and compensation for losses.

Adaptation of the Wyoming (DUNA) Model and the Application of Ultimum Remedium

The proposed Legal Wrapper policy is directly inspired by the success of the U.S. State of Wyoming through its DUNA (Decentralized Unincorporated Nonprofit Association)

legislation. Wyoming has effectively "tamed" DAOs by recognizing their existence while imposing a strict requirement: each DAO must appoint a Registered Agent domiciled in Wyoming. If a DAO violates the law, legal action is directed against the agent. This model can be adapted in Indonesia as part of the transformation of the national criminal justice system toward a more progressive and responsive legal framework.

To enforce the Legal Wrapper mandate in Indonesia, a strict sanction as a last resort (ultimum remedium) is required. Given that DAOs generally have no physical assets in Indonesia, ordinary monetary fines would be ineffective. Therefore, the legal framework must grant authority to the Ministry of Communication and Information Technology to order access termination (blocking) of DAO-supporting infrastructure.

This blocking mechanism would be implemented intelligently. Authorities cannot realistically block a global blockchain network due to its decentralized nature, but they can block front-end interfaces (websites), RPC nodes (connecting servers), and Domain Name System (DNS) services that link DAO applications to Indonesian internet users. As a result, DAOs that refuse to adopt a Legal Wrapper would effectively be "killed" within Indonesia's digital space. This approach to combating information technology crimes through access termination is a strategic measure to prevent the escalation of public harm and is fully consistent with the spirit of cross-border data sovereignty embodied in Perppu No. 1 of 2024, under which the state has the right to close access to foreign entities that refuse to comply with national data protection laws.

Conclusion

The Indonesian criminal law system, which requires the existence of a formal legal subject, encounters a structural failure (deadlock) when confronted with DAOs. To address this liability gap, the Proxy Liability mechanism constitutes a legitimate and applicable solution. This mechanism qualifies the Core Developer as a de facto Personal Data Controller and as a criminal law subject. The Core Developer bears personal responsibility for cross-border data crimes because, in factual terms, he or she exercises control over the code architecture (smart contracts) that gives rise to the harm. Law enforcement is operationalized through On-Chain Forensics, namely the tracing of blockchain transaction records up to the point of conversion into fiat currency (via crypto exchanges), thereby removing the perpetrator's anonymity through KYC data and enabling the imposition of criminal sanctions in accordance with Perppu No. 1 of 2024.

Reactive law enforcement efforts alone are insufficient to address the challenges of cross-border jurisdiction. A preventive structural policy formulation is therefore required through the mandate of a Legal Wrapper. This policy obliges every DAO that processes the personal data of Indonesian citizens to appoint a legally incorporated Legal Representative in Indonesia. This formulation is adopted from the Wyoming Decentralized Unincorporated Nonprofit Association (DUNA) model, which provides legal recognition while simultaneously establishing a clear legal touchpoint. As an enforcement instrument (ultimum

remedium), the state is authorized to impose access termination (blocking) on DAO digital infrastructure (websites and DNS) for entities that refuse to comply with this mandate, in order to uphold legal sovereignty and protect the personal data of citizens.

References

Primavera De Filippi dan Aaron Wright, Blockchain and the Law: The Rule of Code (Cambridge: Harvard University Press, 2018), hlm. 112-115.

Pasal 1 Angka 3 dan Pasal 65 Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Yasmirah Mandasari Saragih, Pengantar Hukum Pidana (Transisi Hukum Pidana di Indonesia) (Medan: CV. Tungga Esti, 2022), hlm. 45-50.

Yasmirah Mandasari Saragih, Mengenal Unsur-unsur Pertanggung Jawaban Pidana oleh Subjek Hukum (Medan: Tahta Media, 2024), hlm. 12-18.

Aaron D. Harden, "DAOs and the Proxy Liability Problem," Stanford Journal of Blockchain Law & Policy, Vol. 4, No. 1 (2022), hlm. 8.

Yasmirah Mandasari Saragih, Pengantar Hukum Pidana (Transisi Hukum Pidana di Indonesia) (Medan: CV. Tungga Esti, 2022), hlm. 60.

Yasmirah Mandasari Saragih, "Effect Of Technology Advances On Cybercrime", International Journal Of Civil Engineering And Technology (IJCIET), Vol 9 Issue 11, 2018, hlm. 2830.

Yasmirah Mandasari Saragih, Mengenal Unsur-unsur Pertanggung Jawaban Pidana oleh Subjek Hukum (Medan: Tahta Media, 2024), hlm. 40-45.

Yasmirah Mandasari Saragih, "Application Of Guidelines For Handling Cases Against Corporations As Criminal Actors", IJIRMF, Vol 8 April 2022, hlm. 110-115. Dan Yasmirah Mandasari Saragih, "Corporate Criminal Liability For Criminal Acts Of Corruption", Jurnal Pembaharuan Hukum, Vol 8 Number 1, 2021.

Yasmirah Mandasari Saragih, "Post-Genesis Digital Forensics Investigation", IJSRST, Volume 3, Issue 6, 2017, hlm. 45-49.

Yasmirah Mandasari Saragih, "Criminology Approach In Solving Cyber Crime", Justisi, 2025, hlm. 15.

Yasmirah Mandasari Saragih, “Transformasi System Pidana Indonesia : Dari KUHP Kolonial menuju KUHP Nasional” (Medan: Tahta Media, 2026), hlm. 80-85.

Yasmirah Mandasari Saragih, “Kajian Dalam Penal Policy Dalam Kejahatan Cyber Crime Di Wilayah Hukum Indonesia”, SANKSI, Vol 1, No 1, 2022, hlm. 120-125.

Yasmirah Mandasari Saragih, "Perlindungan Hukum Terhadap Anak Sebagai Pelaku Tindak Pidana", Innovative: Journal Of Social Science Research, Vol. 3 No. 4, 2024, hlm. 3500-3505. (Diadaptasi untuk konteks perlindungan korban data).

Yasmirah Mandasari Saragih, “Reform of Indonesian criminal law reviewed from law number 1 of 2023 about the criminal code”, International journal of sociology and law, 2025, hlm. 50.

Yasmirah Mandasari Saragih, "Penanggulangan Kejahatan Teknologi Informasi (Cyber Crime) Yang Menimbulkan Kegaduhan Dan Permusuhan Melalui Pendekatan Penal Policy Di Wilayah Hukum Polrestabes Medan", Ensiklopedia of Journal, Vol. 5 No.4 Edisi 2 Juli 2022, hlm. 55-60.