Automating data transfer compliance and dispute resolution with smart contracts

Automatización del cumplimiento y resolución de disputas en la transferencia de datos mediante contratos inteligentes

Jersain Zadamig Llamas Covarrubias
https://orcid.org/0000-0003-1965-2415
Universidad de Guadalajara. México
Correo electrónico: jersain.llamas@gmail.com

Recepción: 23 de octubre de 2024
Aceptación: 26 de febrero de 2025

DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Abstract: This article proposes a hybrid framework that integrates technological and legal solutions to automate compliance and dispute resolution in international personal data transfers. The approach leverages smart contracts built on blockchain technology, incorporating standardized contractual clauses (SCC/MCC) and non-fungible tokens (NFTs) to trigger complaint procedures. By involving supervisory authorities as escrow agents, the system ensures transparency, efficiency, and regulatory compliance, thereby overcoming the limitations of traditional methods. Through comparative analysis and a case study, the article demonstrates the viability of a scalable and interoperable solution that enhances data subjects' rights while aligning with the GDPR and other international regulatory frameworks.
Keywords: data transfers mechanisms; cross-border transfer; adequacy decision; appropriate safeguards; smart contracts; blockchain; dispute resolution.

Resumen: Este artículo propone un marco híbrido que integra soluciones tecnológicas y jurídicas para automatizar el cumplimiento y la resolución de disputas en la transferencia internacional de datos personales. La propuesta se fundamenta en la implementación de contratos inteligentes basados en *blockchain* que incorporan cláusulas contractuales estandarizadas (SCC/MCC) y tokens no fungibles (NFTs) para activar procedimientos de reclamación. Al integrar a las autoridades supervisoras como agentes de custodia, el sistema garantiza transparencia, eficiencia y cumplimiento normativo, superando las limitaciones de los métodos tradicionales. A través de un análisis comparativo y un estudio de caso, se demuestra la viabilidad de una solución escalable e interoperable que fortalece los derechos de los titulares de los datos y se alinea con el RGPD y otros marcos regulatorios internacionales.

Palabras clave: mecanismos de transferencia de datos; transferencia transfronteriza; decisión de adecuación; garantías apropiadas; contratos inteligentes; cadena de bloques; resolución de disputas.

Summary: I. *Introduction*. II. *The current state of data transfers*. III. *Smart contracts, enforceable data subject rights, and effective legal remedies for data subjects*. IV. *Smart contracts and automated dispute resolution in data transfers*. V. *Materials and methods*. VI. *Results*. VII. *Discussion*. VIII. *Conclusions*. IX. *References*. X. *Appendices*.

I. Introduction

The General Data Protection Regulation (GDPR) serves as the global reference for the transfer of personal data to third countries. This regulation provides three main pathways for such transfers: First, based on an adequacy decision, where the European Commission determines that a third country, a specific territory, or one or more sectors within that country ensures an adequate level of data protection. Second, transfers can be made using appropriate safeguards, including legally binding agreements, binding corporate rules, standard contractual clauses, approved codes of conduct, or certification mechanisms. Third, specific derogations may apply, such as explicit consent, necessity for contract performance, public interest, legal claims, protection of vital interests, or transfers from public registers intended for open consultation.

These legal instruments aim to guarantee an adequate level of protection for data subjects. In cases where an adequacy decision is absent, the data controller or processor must ensure equivalent protections by implementing appropriate safeguards, granting enforceable rights to the data subject and effective legal remedies in both the EU and third countries. Additionally, international cooperation plays a crucial role in safeguarding personal data across borders.

However, compliance with these mechanisms can be complex and, at times, ineffective. The case of Schrems II (CJEU, C-311/18) highlighted that the Privacy Shield, a key framework between the EU and the US, failed to provide EU citizens with the same legal protections as US citizens when their data was processed by US authorities. This decision found that the framework was incompatible with Article 47 of the EU Charter of Fundamental Rights (CJEU, 2018), which guarantees the right to an effective remedy. Despite ongoing negotiations for a new Trans-Atlantic Data Privacy Framework, a key question remains: should the challenges of cross-border data transfers be ad-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

dressed solely through regulation, or is there a need for a technological-legal solution?

Beyond the concerns of surveillance and potential violations of fundamental rights in third countries, the central issue remains ensuring an adequate level of data protection and providing data subjects with effective mechanisms to exercise their rights in other jurisdictions.

Given this context, this research paper proposes a hybrid solution that bridges the legal and technological realms. It suggests implementing these contractual and binding instruments through smart contracts, enhanced by execution clauses that enable supervisory authorities to intervene in the event of data protection violations. This approach aims to modernize and streamline current mechanisms for data transfers by embedding enforcement and remedy mechanisms directly within the smart contracts. To support this proposal, the paper will first review existing data transfer mechanisms before introducing improvements through the integration of smart contracts. Additionally, an Appendix will present a pedagogical example of a human-readable legal agreement, and a smart contract designed for a data transfer platform.

This study explores how smart contracts can enhance compliance and dispute resolution in cross-border data transfers, addressing the research question of whether these technologies can improve the protection of personal data. The hypothesis is that smart contracts can automate standard contractual clauses, providing more efficient and transparent enforcement mechanisms. While the central argument supports their integration into legal frameworks, a counter-argument acknowledges the technical and regulatory challenges that may limit adoption. The objectives are to propose an interoperable solution for data transfer compliance, assess the role of smart contracts in protecting data subject rights, and evaluate scalability across jurisdictions. The methodology combines a qualitative review of existing frameworks and a prototype-based case study. Structured to introduce the problem, present the solution, and discuss findings, this study is written in a critical-analytical style, grounded in empirical evidence rather than opinion.

II. The current state of data transfers

The transfer of personal data to a third country or an international organization is a common practice, involving exchanges between different entities such as controller-controller, controller-processor, processor-processor, and processor-controller relationships. The first mechanism for enabling such transfers is the adequacy decision (Art. 45, GDPR) adopted by the European

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Commission, which recognizes when a third country or international organization provides an adequate level of data protection (Regulation (EU) 2016/679, 2016). In addition, an axiological study of the decentralized and distributed nature of blockchain was carried out to assess its potential conflict with regulations, specifically regarding the identification of data controllers for the purposes of transfer and transmission of information. However, once controllers are clearly identified, either through a Distributed Ledger Technology (DLT) framework or by established agreements, this issue could be resolved, ensuring compliance with data protection standards even within decentralized networks (Llamas Covarrubias, 2021).

In the absence of an adequacy decision, appropriate safeguards must be used. According to Article 46 of the GDPR, these include instruments such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), Codes of Conduct, Certification Mechanisms, Ad hoc Contractual Clauses, and International Agreements/Administrative Arrangements (Regulation (EU) 2016/679, 2016).

From an Ibero-American perspective, the use of Model Contract Clauses (MCC), which are comparable to the SCCs in Europe, serves to ensure compliance with the data protection laws of the exporting country. These clauses allow data subjects to be considered third-party beneficiaries, granting them the right to claim compensation if contractual duties are breached by the data importer. Although the data subject is not a direct signatory of the contract between the exporter and importer, they can exercise their rights, creating an autonomous data protection regime without requiring national-level legal convergence (REDIPD, 2022).

Binding Corporate Rules (BCRs), as specified in Article 44 GDPR, allow groups of companies or enterprises engaged in joint economic activities to transfer personal data under a unified set of data protection policies (Regulation (EU) 2016/679, 2016; EDPB, 2022). Additionally, Article 46 emphasizes the role of Codes of Conduct, prepared by associations representing categories of controllers or processors, as another appropriate safeguard (Regulation (EU) 2016/679, 2016; EDPB, 2021).

Certification mechanisms (Article 42(2)) offer another avenue for data transfers. These voluntary schemes provide adequate guarantees through a binding audit methodology, allowing controllers or processors outside the European Economic Area (EEA) to demonstrate compliance with EU standards (Regulation (EU) 2016/679, 2016; EDPB, 2023). Similarly, ad hoc contractual clauses can be crafted between data exporters and importers, ensuring compliance with essential transfer requirements and offering the flexibility to adapt to specific transfer needs (Regulation (EU) 2016/679, 2016).

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Lastly, international agreements or administrative arrangements, under Article 46(2)(a), enable public bodies within the EEA to transfer personal data to public bodies in third countries without prior authorization from a Supervisory Authority, provided these arrangements are legally binding and enforceable (Regulation (EU) 2016/679, 2016; EDPB, 2020).

In situations where neither adequacy decisions nor appropriate safeguards are available, Article 49(1) allows for limited derogations. These derogations apply in exceptional circumstances, such as when transfers are occasional and necessary, and should be used only as a last resort (Regulation (EU) 2016/679, 2016; EDPB, 2018, pp. 3-8).

A comprehensive analysis of the entire data lifecycle is essential, encompassing stages from collection to conservation, cancellation, and the general aspects of access. This includes the use of data, its transfer to competent authorities, and adherence to recommendations from the data protection regulatory body (Hernández González, 2018). Before initiating any transfer, conducting a Transfer Impact Assessment (TIA) is crucial. The European Data Protection Board (EDPB) recommends several steps for data exporters: mapping all data transfers, verifying the transfer mechanism, assessing the legal framework of the third country, identifying supplementary measures, taking formal procedural steps, and periodically re-evaluating the level of protection (EDPB, 2021, pp. 3-5).

1. Comparative analysis of cross-border data transfer regulations

The international regulatory landscape for cross-border data transfers is highly heterogeneous, with jurisdictions adopting diverse approaches to data localization, transfer restrictions, and compliance mechanisms. This section provides a comparative analysis of key jurisdictions, summarizing their legal frameworks, transfer requirements, and data residency rules (see Table 1). By highlighting these differences, we underscore the challenges posed by divergent regulatory regimes and lay the groundwork for discussing how smart contracts can automate compliance and streamline cross-border data governance. This analysis is based on Tang (2023, pp. 224-239), who provides a comprehensive overview of global data transfer regulations.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Table 1. Comparative of cross-border data transfer regulations

Jurisdiction	Legal Framework / Regulatory Instrument	Key Transfer Restrictions and Data Residency Requirements	Remarks / Implications
Argentina	Ley 25.326 de Protección de los Datos Personales	Requires explicit consent and adequate protection measures; prior notification to data subjects is often needed.	Emphasizes safeguarding individual rights via contractual and consent mechanisms.
Australia	Privacy Act 1988; Australian Privacy Principles (APPs)	Transfers allowed only to jurisdictions with comparable protection or through binding contractual safeguards; strict rules for government data.	Provides flexibility for commercial entities, yet imposes stringent standards for public sector data.
Canada	PIPEDA; Provincial laws (e.g., BC's FOIP, Nova Scotia's PIPA, Quebec Privacy Act)	Public institutions must store data domestically; private sector transfers are permitted if contractual commitments ensure comparable protection.	Dual approach with region-specific requirements necessitating tailored compliance strategies.
China	Personal Information Protection Law; Cybersecurity Law	Mandates local data storage for critical information; cross-border transfers require security reviews, certifications, or standard clauses.	Reflects high state control and rigorous review, challenging technological integration.
Colombia	Ley 1581 de 2012	Transfers permitted only if the destination ensures an adequate protection level or if explicit consent is obtained.	Leverages contractual safeguards as a primary compliance tool.
Croatia	Implementation Act of GDPR	Requires adequacy decisions or approved safeguards (SCCs, BCRs); some transfers need prior DPA approval.	As an EU member, it closely aligns with GDPR standards.
EU and EEA	General Data Protection Regulation (GDPR)	Strict conditions via adequacy decisions, SCCs, and BCRs; often requires DPA oversight and sometimes prior authorization.	Provides a uniform, high-standard framework for data protection.
Hong Kong	Personal Data (Privacy) Ordinance	Transfers allowed if recipient provides comparable protection, typically secured via contractual obligations.	Balances local standards with international practices.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

India	IT Rules; Upcoming Personal Data Protection Bill	Sensitive data transfers restricted to jurisdictions with adequate protection or require explicit consent and additional safeguards.	Increasing emphasis on data localization and explicit consent mechanisms.
Iceland	Act No. 90/2018 on Data Protection	Transfers permitted to jurisdictions with adequate protection, in line with GDPR-like standards.	EU/EEA alignment ensures rigorous data protection requirements.
Indonesia	Regulation No. 82 concerning Electronic System Operation	Mandates local storage for public service operators; transfers require certifications and, in some cases, prior regulatory approval.	Strong focus on local IT infrastructure and data localization.
Israel	Privacy Protection Act Nos. 5741/1981 and 5752/1992	Transfers allowed only if the recipient ensures protection levels comparable to domestic law or with explicit consent and contractual agreements.	Uses robust contractual frameworks to safeguard data.
Japan	Act on the Protection of Personal Information (APPI)	Transfers permitted if the recipient has an equivalent protection system or via approved contractual measures.	Emphasizes adequacy assessments and standardized clauses.
Lesotho	Data Protection Act 2011	Permits transfers if recipients adhere to similar data processing principles or if explicit consent is provided.	Focuses on core data protection principles.
Madagascar	Law No. 2014–038	Transfers are allowed only if the destination ensures a sufficient level of protection or with explicit consent.	Involves exceptional approval processes in certain cases.
Macedonia	Law on Personal Data Protection 2020	Permits transfers only if the third country provides adequate protection or through DPA-approved safeguards.	Reflects EU adequacy models and alignment with European standards.
Mauritius	Data Protection Act 2017	Transfers restricted unless recipient ensures comparable safeguards or explicit consent is obtained.	Balances flexibility with robust protective measures.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Malaysia	Personal Data Protection Act 2010	Transfers allowed only to jurisdictions with adequate protection, or if explicit consent and due diligence are in place.	Focuses on protecting sensitive personal data via rigorous safeguards.
Mexico	Federal Law on Protection of Personal Data Held by Private Parties 2010	Requires notification, consent, and contractual commitments for transfers; affiliated companies may be exempt from consent requirements.	Emphasizes consumer rights and data subject protections.
Montenegro	Law on Protection of Personal Data (various amendments)	Transfers permitted only to countries with adequate protection or via approved contractual clauses and DPA oversight.	Closely aligned with EU/EEA requirements.
Morocco	Act No. 09–08 on the Protection of Individuals regarding Data Processing	Transfers restricted unless the recipient meets strict protection criteria or explicit authorization is granted by the DPA.	Involves rigorous oversight and justification for transfers.
Monaco	Data Protection Law No. 1.165 (with subsequent amendments)	Allowed only to jurisdictions with equivalent protection; contractual safeguards are essential.	Harmonizes with European data protection norms.
New Zealand	Privacy Act 2020	Transfers permitted if the recipient country offers an adequate level of protection; recognized as adequate by the EU.	Provides a stable, high-standard data protection framework.
Nigeria	National guidelines; Proposed Personal Data Protection Bill 2020	Imposes local storage for certain data types; transfers subject to strict regulatory conditions and, in some cases, explicit consent.	Emphasizes both consumer and government data security.
Pakistan	Proposed Personal Data Protection Bill 2020	Sensitive data transfers allowed only to recognized jurisdictions, with explicit consent and regulatory approval required.	Focuses on safeguarding sensitive sectors (e.g., banking, defense).
Peru	Ley núm. 29733 - Ley de Protección de Datos Personales	Transfers permitted only if the destination provides adequate protection or with the data subject's consent secured by written agreements.	Leverages contractual measures as a key compliance tool.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Singapore	Personal Data Protection Act 2012; Regulations 2014	Requires recipients to offer a protection standard comparable to the PDPA, enforceable by legally binding contracts.	Highlights the centrality of contractual obligations for cross-border transfers.
South Africa	Protection of Personal Information Act	Transfers allowed only if the recipient provides a comparable level of protection or with explicit data subject consent.	Balances data protection with commercial flexibility.
Switzerland	Federal Act on Data Protection (FADP)	Cross-border transfers permitted only to jurisdictions with adequate protection or via approved contractual clauses.	Maintains high protection standards similar to the EU/EEA.
Serbia	Law on Personal Data Protection N°97/08	Transfers require assurance of adequate protection or prior DPA authorization for sensitive data.	Aligns with European data protection standards.
Seychelles	Data Protection Act of 2003	Transfers are restricted if likely to contravene data protection principles; DPA may issue prohibition notices.	Emphasizes precaution and strict regulatory oversight.
South Korea	Personal Information Protection Act (PIPA)	Requires prior notification and explicit consent for cross-border transfers; strict enforcement mechanisms in place.	Known for its rigorous framework and strong enforcement.
Russia	Amendments to the Data Protection Act (e.g., No. 152 FZ)	Mandates local storage of Russian citizens' data; transfers permitted only to jurisdictions with an adequate level of protection.	Enforces strict local storage rules; recent cases underscore regulatory vigilance.
Kingdom of Saudi Arabia (KSA)	Sector-specific regulations and local practices (no single comprehensive law)	Generally requires local server deployment and pre-transfer approval by telecom authorities; cross-border transfers are highly scrutinized.	High sensitivity regarding data sovereignty and national security.
Trinidad and Tobago	National Privacy Protection Legislation	Transfers require prior authorization and must ensure adequate protection for both public and private sector data.	Emphasizes rigorous approval procedures to safeguard data.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Tunisia	Applicable Data Protection Law (e.g., Law No. 2004-63)	Transfers allowed only with adequate safeguards or explicit consent; often modeled after European standards.	Reflects a growing commitment to robust data protection measures.
Ukraine	National Data Protection Law	Cross-border transfers permitted only to jurisdictions with adequate protection or via stringent contractual safeguards; may require DPA approval.	Increasingly aligning with EU standards amid reform efforts.
Uruguay	Data Protection Law (EU-recognized adequacy)	Generally allows transfers provided that the recipient ensures a protection level comparable to domestic standards.	Serves as a benchmark for data protection in Latin America.
United States	Sectoral regulations (e.g., HIPAA, DFARS for government data)	Relies primarily on contractual agreements; specific restrictions apply to government cloud services with mandated local storage.	Fragmented regulatory approach offers flexibility yet challenges uniformity.
Vietnam	Decree on Management, Provision, and Use of Internet Services and Information Content Online (Decree 72)	Requires local IT infrastructure and data centers; cross-border transfers subject to regulatory approval and compliance with local storage mandates.	Emphasizes local data storage and tight government oversight.

SOURCE: own elaboration based on Tang (2023, pp. 224-239).

This table 1 provides a holistic view of the regulatory environment affecting cross-border data transfers in key jurisdictions. It can serve as a foundation for further discussion on how smart contracts may be designed to automatically enforce these diverse legal requirements, streamline compliance processes, and ultimately enhance international data governance.

Taken together, the heterogeneous regulatory landscape underscores both the challenges and opportunities for employing smart contracts in global data transfers. Evaluating the scalability and legal viability of the proposed solution across diverse legal frameworks, from the stringent requirements of the GDPR to more flexible, sector-specific regimes, reveals that a standardized, interoperable approach is essential. By integrating pre-approved contractual templates and robust supervisory oversight mechanisms, the solution can potentially harmonize compliance processes on a global scale. Nonetheless, fur-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

ther empirical research is necessary to address jurisdiction-specific obstacles and ensure that the technological framework remains adaptable to evolving legal standards, thereby fostering a resilient and legally sound model for international data governance.

2. Additional perspectives on blockchain and data transfer mechanisms

In the context of cross-border data transfers, public (permissionless) blockchain networks present significant challenges. Regulatory bodies such as the CNIL have noted that, due to the global distribution of participants and miners, personal data may be processed in jurisdictions outside the European Union, often in regions without an adequacy decision. The decentralized nature of these platforms renders traditional safeguards (such as standard contractual clauses or binding corporate rules) largely ineffective. This has led to recommendations favoring the use of permissioned blockchains, where data controllers can exercise tighter oversight of miner locations and data flows (Voss 2021, p. 99).

Furthermore, many industries, including banking and healthcare, are currently hampered by fragmented data management systems, with each institution maintaining its own database. By contrast, a unified blockchain ledger that serves multiple parties can significantly streamline these processes. Such a shared ledger minimizes the administrative burdens associated with disparate systems, accelerates data transfers, and provides all participants with a single, reliable source of truth (Anusha *et al*., 2024, p. 99). This approach not only enhances operational efficiency but also supports the integrity and transparency of data governance.

Complementing these technological advancements, the Data Act introduces a regulatory framework that further bolsters the potential of smart contracts in data sharing. In this framework, smart contracts are defined as self-executing programs on electronic ledgers that enforce predetermined data sharing conditions automatically. The Data Act emphasizes interoperability by establishing essential requirements for smart contracts, such as robust design, secure termination protocols, comprehensive data archiving, and stringent access controls, to ensure that data transfer conditions are consistently met (EU Blockchain Observatory and Forum, 2022, pp. 20-21). This regulatory perspective not only enhances the technical efficiency of automated processes but also ensures that these innovations align with established legal safeguards, paving the way for more reliable and secure international data transfers.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

III. Smart contracts, enforceable data subject rights, and effective legal remedies for data subjects

The potential of smart contracts to enforce data subject rights and offer effective legal remedies is a growing area of interest in both the legal and technological fields. To fully grasp this intersection, it is essential to first understand the fundamentals of blockchain technology. According to Bashir (2020, pp. 65-66), blockchain can be defined as:

- Layman's definition: Blockchain is a continuously expanding, secure, shared record-keeping system in which each participant holds a copy of the records. These records can only be updated if all parties involved in the transaction agree.
- Technical definition: Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable, and updatable only through consensus among participants.

Blockchain networks are generally categorized into three types: Public (Permissionless), Private (Permissioned), and Consortium networks. Public blockchains are open to anyone and are updated through consensus mechanisms, while Private blockchains restrict access and validation to pre-selected participants. Consortium blockchains blend elements of both, allowing a hybrid model of participation and control (Upadhyay, 2019, pp. 65-66). This technology is part of the broader category of Distributed Ledger Technology (DLT), which involves the replication, sharing, and synchronization of digital transactions across various locations. Not all DLTs, however, are decentralized, and this distinction is key to understanding the regulatory challenges posed by blockchain (Prusty, 2018, p. 28).

With a solid grasp of blockchain technology, the next logical question is: Do data protection regulations apply to blockchain networks? Some argue that blockchain-based data is anonymized and thus falls outside the scope of data protection laws. However, this argument is flawed. Anonymization must ensure that data cannot be re-identified, but the cryptographic techniques used in blockchain (e.g., encryption, hashing) often only achieve pseudonymization, which involves indirect identifiers. Pseudonymized data still falls under data protection regulations, such as the GDPR, as it can potentially be linked back to identifiable individuals (CNIL, 2018, p. 5).

A core challenge arises from the inherent immutability of blockchain, which complicates the exercise of data subject rights, such as the right to erasure, rectification, or the right to be forgotten. This is especially problematic

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

in public and permissionless blockchains, where the ledger is open to participants globally, making cross-border data transfers unavoidable. While private and consortium blockchains offer more control over data, facilitating compliance through mechanisms such as standard contractual clauses (SCCs) and binding corporate rules (BCRs), implementing such safeguards in public blockchains remains difficult due to the decentralized nature of these networks (Bacon *et al*., 2017, p. 47).

While blockchain's immutable ledger presents unique challenges, smart contracts provide an innovative solution to enforce data subject rights. A smart contract is essentially self-executing code stored on the blockchain, which can automatically enforce contractual terms without the need for intermediaries (Ramamurthy, 2020, p. 23). In the context of data protection, smart contracts could play a pivotal role in automating and streamlining the enforcement of data subject rights, especially in cases involving data transfers or breaches.

For instance, the EU's Data Act (Regulation (EU) 2023/1232, 2023) outlines key requirements for smart contracts, such as robustness, safe termination, data archiving, and access control. These essential features can be harnessed to create a robust framework for resolving disputes related to data subject rights. By embedding these safeguards into smart contracts, a technological-legal mechanism could be established to facilitate faster, more efficient resolution of contractual disputes.

Imagine an SCC that is transformed into a smart contract. The exporter and importer sign the SCC, and the smart contract includes an escrow clause managed by a supervisory authority. If a dispute arises —triggered by a data subject— the smart contract would automatically activate the appropriate safeguards, transferring the matter to the relevant supervisory authority or a designated tribunal for resolution. This would not only expedite the process but also provide legal certainty in enforcing data protection rights in a decentralized environment.

The decentralized platform Kleros serves as a compelling example of how blockchain technology can facilitate dispute resolution. Kleros allows parties to enter into smart contracts with dispute resolution clauses, which are then adjudicated by a decentralized court. For instance, if Alice and Bob sign a Kleros Escrow contract and a dispute arises, the case is judged by the Kleros court, and the judgment is executed via the smart contract, with funds in escrow being transferred accordingly (Lesaege, George and Ast, 2021, p. 5).

Although Kleros requires the use of cryptocurrencies or tokens, the agility and automation of its dispute resolution system are noteworthy. For this article's proposal, the idea is not to create decentralized courts but to apply similar

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

mechanisms within existing legal frameworks, such as supervisory authorities, to accelerate the resolution of disputes involving data subject rights. Kleros Themis Project, which aims to expand dispute resolution beyond the blockchain, could serve as a model for integrating smart contract-based dispute resolution mechanisms into traditional legal settings (Ast, 2020).

In sum, smart contracts offer a promising path toward more efficient enforcement of data subject rights in an increasingly decentralized digital landscape. By combining the automation of smart contracts with the legal safeguards of data protection regulations, it is possible to design a system that efficiently resolves disputes while maintaining compliance with regulatory standards. The example of Kleros demonstrates that blockchain-based dispute resolution is not only feasible but also practical, and with the proper regulatory oversight, it can be adapted to protect data subjects' rights.

IV. Smart contracts and automated dispute resolution in data transfers

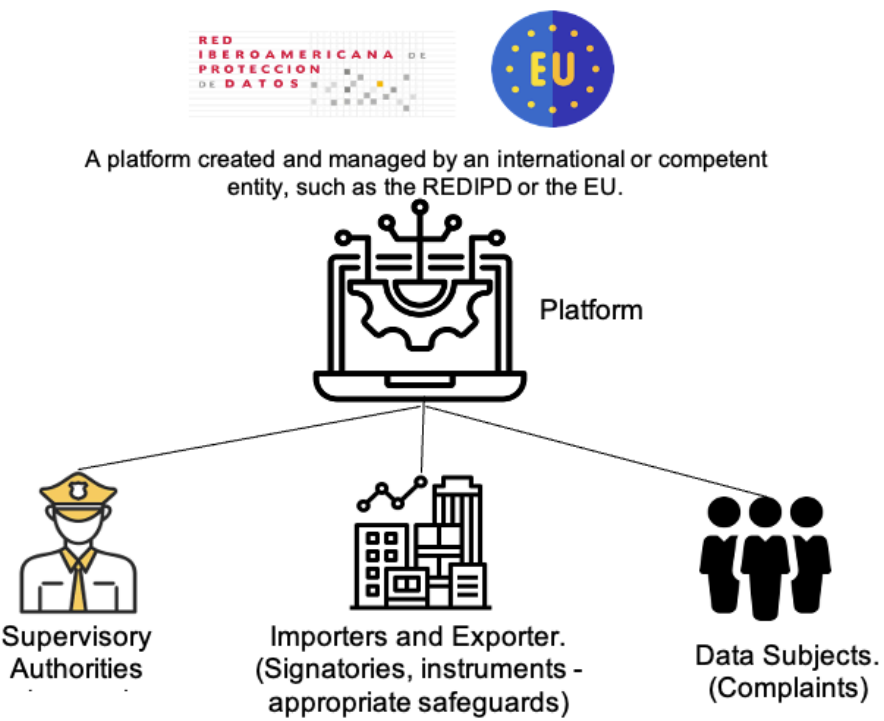
The process by which the acceptance or refusal to authorize the transfer of data to third parties is communicated has traditionally followed standardized legal procedures (Ocampo Muñoa, 2019: 16). However, imagine a more operational and automated approach to Standard Contractual Clauses (SCCs) or Model Contractual Clauses (MCCs), where the exporter and importer not only sign the agreement, but the dispute resolution process is streamlined through the use of smart contracts. In this proposed system, a platform managed by the EU or an international organization such as the RIDPDB could transform SCCs or MCCs into smart contracts that automate compliance and dispute resolution. These contracts would incorporate an escrow clause, involving competent supervisory authorities to ensure that disputes are resolved in a transparent and efficient manner. Additionally, the activation of the dispute process would rest in the hands of the data subject, who could initiate a complaint using a compliant token, such as a Non-Fungible Token (NFT), which would be issued upon signing the SCC or MCC. This token would serve as a unique digital trigger, allowing the data subject to exercise their rights in a secure and traceable manner, while also ensuring that the entire process remains transparent and compliant with regulatory standards.

The creation of a secure and interoperable platform is critical. Once this platform is in place, the following steps would guide its functionality:

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

1. Platform management: The platform would be operated by the EU or an international body such as the REDIPD. Each supervisory authority would maintain an account (escrow). Exporters and importers must register with signing rights, while data subjects would register with permissions to lodge complaints.

Graphic 1.



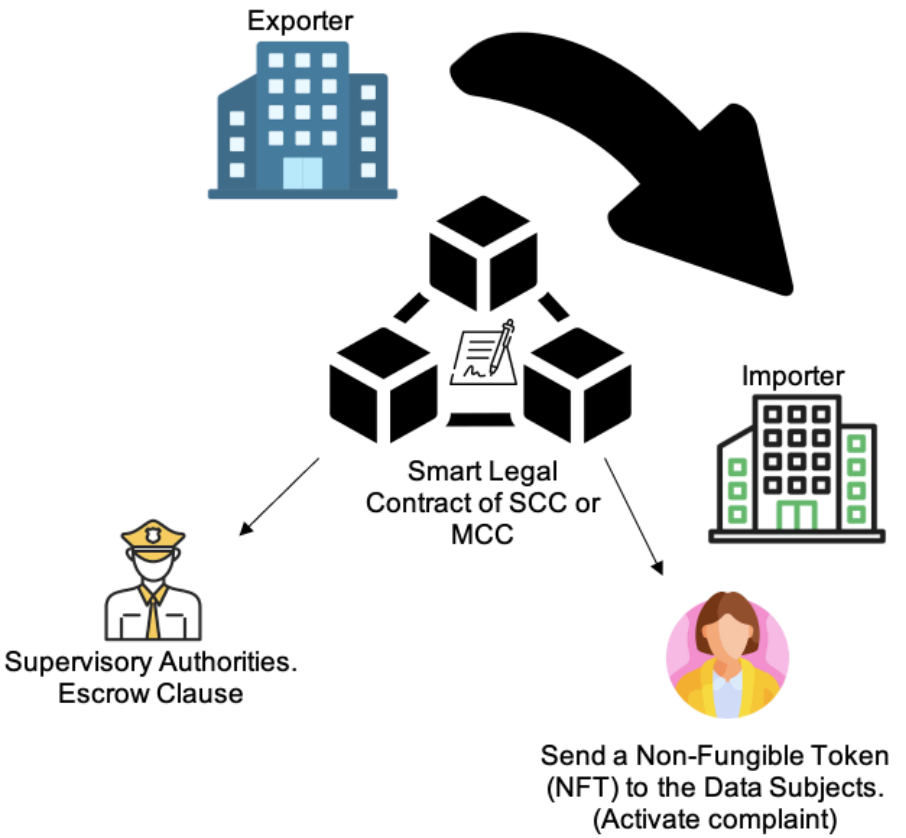
Graphics made by Elzicon, Pixel perfect, Iconjam, Freepik, surang, IconBaandar, on flaticon.com

2. SCC/MCC templates: Templates of SCCs or MCCs approved by competent authorities would be available on the platform for exporters and importers to use.

3. Execution of smart contracts: Once the appropriate transfer mechanism is selected, the exporter and importer would execute the smart contract on the platform. The supervisory authority would act as escrow. Upon signing the contract, an NFT would be sent to the data subject, which they could later use as a trigger for complaint.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Graphic 2.



Graphics made by Elzicon, itim2101, Anggara, Pixel perfect, Iconjam, Freepik, surang, Icon-Baandar, muhrzkifauzi, on flaticon.com

4. Complaint mechanism: If the data subject believes their rights under data protection laws have been violated, they could activate the complaint and resolution mechanisms on the platform by using the NFT.

5. Dispute resolution: When the complaint mechanism is activated, the platform would automatically forward the case to the competent supervisory authority, depending on whether the exporter or importer violated the data protection regulation.

6. Ruling enforcement: After the prescribed period, the supervisory authority would issue a ruling, which would carry legal validity within the relevant jurisdiction.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

This proposed system integrates smart contracts and NFTs to automate and streamline the enforcement of data protection rights, offering a more efficient and interoperable solution for cross-border data transfers. By leveraging smart contracts, the resolution of disputes can be expedited while maintaining compliance with applicable laws, providing a robust framework for international data governance.

To demonstrate the proposed system's practical application, consider a case study involving cross-border data transfer under the GDPR framework. A France-based financial institution (Exporter) needs to transfer customer transaction data to a U.S.-based analytics provider (Importer) for risk assessment and fraud detection. Under the GDPR, such transfers require appropriate safeguards, typically implemented through Standard Contractual Clauses (SCCs). However, ensuring ongoing compliance and resolving disputes over data protection obligations remain significant challenges.

The proposed smart contract-based system addresses these challenges through the following structured steps:

1. Platform Management and Registration
- The financial institution and analytics provider register on a secure data transfer platform, overseen by the French Data Protection Authority (CNIL) and the U.S. Federal Trade Commission (FTC).
- The European Data Protection Board (EDPB) maintains an escrow account to handle disputes between EU and non-EU entities.
- Data subjects (bank customers) are granted permissions to file complaints in case of data rights violations.

2. Use of SCC Templates and Smart Contract Execution.
- Instead of traditional SCC documents, the exporter and importer select a pre-approved smart contract SCC template from the platform.
- The smart contract automatically verifies compliance, ensuring that the U.S. importer adheres to GDPR requirements, such as encryption, storage limitations, and access control policies.
- The contract executes automatically, embedding SCC obligations into immutable blockchain records.

3. Issuance of NFTs to Data Subjects.
- Upon execution, an NFT (Non-Fungible Token) is issued to each affected data subject as proof of SCC-compliant data transfer.
- The NFT serves as a digital trigger, enabling data subjects to exercise their rights in case of disputes.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

4. Complaint Mechanism Activation

- One month later, the financial institution detects unauthorized secondary data processing by the U.S. analytics provider, violating the SCC terms.
- Affected data subjects use their NFTs to file formal complaints via the platform.
- The platform automatically verifies the complaint and notifies both the CNIL and the FTC, ensuring regulatory oversight and coordinated enforcement.

5. Dispute Resolution and Ruling Enforcement

- The CNIL, in coordination with the EDPB, investigates the importer's compliance status.
- The ruling confirms a GDPR violation, triggering an automated financial penalty encoded within the smart contract.
- The importer's permissions are revoked, and the FTC is notified to take enforcement action under U.S. sectoral privacy laws, ensuring alignment with the regulatory framework applicable in both jurisdictions.

This case study illustrates the real-world applicability of the proposed system by automating SCC compliance, enabling direct data subject intervention via NFTs, and integrating supervisory authorities into the dispute resolution process. By embedding SCCs into self-executing smart contracts, the solution mitigates legal uncertainties, enforcement delays, and administrative burdens.

Furthermore, the model is scalable beyond financial services, with potential applications in healthcare, e-commerce, and cloud computing, particularly in jurisdictions where data protection frameworks require strict cross-border transfer compliance. As privacy regulations continue to evolve, this approach provides a flexible, legally enforceable, and technologically robust framework for international data governance.

1. Governance, and security considerations for blockchain networks in cross-border data transfers

The transfer of personal data to countries lacking a data protection regime or that do not provide an adequate level of protection is a critical issue that requires careful consideration (Cubillos Vélez, 2017, pp. 30, 45). It is crucial for blockchain network participants to carefully consider several legal and governance aspects before embarking on a blockchain project. A well-defined legal structure, clear responsibilities, and a transparent governance model

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

are essential to ensuring that all participants understand how the network operates. The following considerations are critical in the early stages of any blockchain project (WEF, 2020):

- Participants must decide how the blockchain network will be structured from a legal perspective. Key questions include whether the network will operate under a legal entity, such as a business or partnership, and whether there will be one or more network operators. Ownership and control of the network must be clearly defined, including how participants will join the network and take ownership.
- Clear legal documentation outlining the network's structure, accountability, and governance is essential. Participants must establish whether the network will have a legally enforceable rulebook or terms of use that participants must agree to. Alternatively, separate contracts between participants and the network operators may be considered. Defining the rights and obligations of participants is crucial, particularly if there are different classes of participants with varying levels of rights and responsibilities. Additionally, participants must determine whether there will be a fee to join the network and how this fee will be structured.
- Beyond the legal and governance aspects, privacy and security are critical components in the design of any blockchain network. Key measures include configuring on-chain/off-chain data storage to ensure sensitive information is not directly stored on the blockchain. Storing only hashed data, implementing role-based access control, and using techniques such as zero-knowledge proofs to allow participants to verify their knowledge of a value without revealing the value itself are also essential security practices (WEF, 2019). Furthermore, encrypting data before sharing it on the blockchain allows for analysis without the need for decryption, adding an additional layer of protection.

By addressing these considerations early on, blockchain network participants can create a secure, transparent, and legally sound platform that fosters trust among participants and ensures compliance with relevant legal frameworks.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

2. Legal and technical challenges of smart contract implementation for international data transfers

The implementation of smart contracts in cross-border data transfers presents several legal and technical challenges that must be addressed to ensure compliance, enforceability, and operational efficiency. While these contracts offer automation and transparency, their integration into existing legal frameworks presents significant complexities.

From a legal perspective, one of the primary challenges is regulatory uncertainty. The applicability of smart contracts under data protection regulations varies across jurisdictions. While the GDPR acknowledges mechanisms such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) as appropriate safeguards for international data transfers, it does not explicitly recognize smart contracts as a regulatory compliance tool. This ambiguity raises concerns regarding their legal validity unless formally integrated into data protection frameworks.

Another critical issue is jurisdictional enforcement. Blockchain networks are inherently global, operating beyond national borders. This decentralized nature complicates the determination of competent jurisdiction for resolving disputes and enforcing compliance. Unlike traditional legal agreements that fall under national contract laws, smart contracts require additional oversight or hybrid enforcement mechanisms to bridge the gap between automation and legal intervention.

Furthermore, revocability and amendability pose additional challenges. Smart contracts are designed to be immutable once deployed on the blockchain, ensuring that contractual terms cannot be altered post-execution. However, data protection laws, such as GDPR Article 17 (Right to Erasure), require that personal data be rectifiable or erasable upon request. The inherent immutability of smart contracts raises compliance concerns, necessitating technical solutions that allow modifications while maintaining data integrity and regulatory adherence.

On the technical side, one of the main challenges is oracles and external data dependencies. Smart contracts rely on external data sources, known as oracles, to trigger execution conditions (e.g., breach notifications, regulatory compliance status). These dependencies introduce vulnerabilities such as data manipulation risks and oracle failures, potentially compromising contract execution and reliability. Ensuring that oracles provide accurate and tamper-proof information is crucial for the integrity of smart contract enforcement.

Another significant consideration is scalability and cost efficiency. Public blockchain networks, particularly those based on proof-of-work (PoW)

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

or proof-of-stake (PoS) mechanisms, may encounter performance bottlenecks and high transaction fees, making them less viable for large-scale data transfers. Addressing these issues requires the use of optimized architectures, such as permissioned blockchains or layer-2 scaling solutions, which balance efficiency with compliance.

Lastly, interoperability with existing legal systems remains a challenge. Traditional data transfer frameworks rely on human-readable agreements that require interpretation by legal professionals. Converting these legal documents into machine-executable smart contracts introduces semantic and interpretive challenges, requiring a carefully designed legal-technical alignment. Without standardized methodologies to bridge legal language and smart contract execution logic, discrepancies in enforcement could arise.

By tackling these legal and technical hurdles, the proposed model seeks to improve the practicality of smart contracts in cross-border data governance. By combining smart contract automation with regulatory oversight mechanisms, it ensures compliance, enforceability, and adaptability, effectively bridging the gap between technological innovation and established legal safeguards.

3. Ensuring compliance in decentralized environments

While smart contracts enable automated execution based on predefined conditions, their enforceability in decentralized environments is not absolute due to potential technical failures or legal disputes. To address these challenges, this framework incorporates three layers of compliance assurance:

1) *Regulatory Oversight and Auditing by Supervisory Authorities:* Despite the automation of contractual enforcement, smart contracts operate within a regulated platform supervised by data protection authorities. These authorities act as guarantors, ensuring that all transactions comply with applicable legal frameworks. In the event of a dispute, they retain the authority to review, intervene, and enforce compliance through legally binding decisions.
2) *Technical Enforcement via Oracles and Multi-Signature Mechanisms:* To mitigate the risk of non-execution due to technical failures or malicious manipulation, the platform integrates decentralized oracles that validate key contractual events. Additionally, multi-signature mechanisms allow supervisory authorities to intervene manually in cases where automatic execution fails or where dispute resolution requires human oversight.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

3) *Hybrid Dispute Resolution Mechanisms:* The proposed system combines automated enforcement with legally recognized dispute resolution processes. In cases where a smart contract is improperly executed or contested, the platform facilitates arbitration through mechanisms such as decentralized adjudication systems (e.g., Kleros) or traditional legal proceedings overseen by specialized data protection courts.

By embedding these safeguards, the proposed framework ensures that smart contracts for data transfers remain enforceable, resilient, and compliant with international regulatory standards. This approach not only strengthens legal certainty but also enhances the practical viability of decentralized compliance mechanisms in cross-border data governance.

V. Materials and methods

This section outlines the materials and methods proposed for implementing a technological-legal framework designed to enhance data transfers while ensuring enforceable data subject rights and effective legal remedies. This hybrid approach leverages smart contracts within a secure and interoperable platform to expedite dispute resolution and ensure compliance with data protection regulations.

1. Blockchain and Distributed Ledger Technology (DLT)

We propose utilizing a permissioned blockchain or DLT network as the foundational infrastructure for the data transfer platform. A permissioned blockchain ensures control over network participants, accountability, and the ability to enforce compliance with legal frameworks. This structure will maintain data integrity and immutability, while offering a flexible model to support private, public, or consortium-based networks depending on the requirements of stakeholders. By utilizing a permissioned network, the system addresses concerns about governance and control, which are essential for managing sensitive data transfers and ensuring compliance with data protection laws.

2. Smart contracts for data transfers

Smart contracts will be central to automating and validating the data transfer process. These contracts will be based on approved Standard Contractu-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

al Clauses (SCCs) or Model Contract Clauses (MCCs), which are established safeguards for international data transfers under data protection regulations such as the GDPR. Written in Solidity, a programming language specifically designed for smart contracts on blockchain platforms, these contracts will allow for automated execution and transparent validation of the data transfer process, reducing the need for intermediaries and expediting compliance with legal obligations.

3. Supervisory authority integration

The integration of supervisory authorities as escrow agents or guarantors within the platform will facilitate real-time oversight and dispute resolution. Supervisory authorities, such as national data protection bodies, will play a key role in ensuring that data transfers comply with applicable legal frameworks. The involvement of these authorities will provide data subjects with an efficient and streamlined mechanism to exercise their rights and escalate complaints. This approach not only enhances transparency but also reinforces the enforceability of data protection rights in cross-border transfers.

4. Non-Fungible Token (NFT) trigger

Upon the execution of a smart contract between the data exporter and importer, a Non-Fungible Token (NFT) will be issued to the data subject. This NFT will serve as a unique trigger, enabling the data subject to initiate a complaint or dispute resolution process if they believe their rights have been violated. The use of NFTs ensures traceability and accountability, as each token is immutably linked to a specific transaction, allowing for transparent verification of complaints. This mechanism strengthens the legal enforceability of data subject rights by leveraging the automation and immutability of blockchain technology.

5. Data Protection Impact Assessment (DPIA)

Prior to processing any data or deploying the platform, a Data Protection Impact Assessment (DPIA) will be conducted by the data controller. This assessment will evaluate the potential risks to data subjects and ensure that the platform adheres to relevant data protection regulations, such as the GDPR. Supervisory authorities may also participate in the DPIA process to guarantee that the system complies with global data protection standards and mitigate any legal or ethical concerns related to data privacy and security.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

6. Secure and Interoperable Platform

The platform will be designed with robust security and privacy mechanisms to ensure data protection throughout the entire transfer process. On-chain/off-chain configurations will be employed to securely store sensitive data, with only hashed or pseudonymized data being retained on the blockchain to mitigate privacy risks. Additional measures, such as encryption, role-based access controls, and selective obfuscation techniques, will further enhance the security of data transfers. These features will ensure compliance with legal documentation requirements by clearly defining the roles, rights, and obligations of all participants, while maintaining the integrity and confidentiality of the data.

7. User-Friendly Interface

Although the backend infrastructure of the platform will incorporate advanced technologies, the frontend will be designed to prioritize usability. A user-friendly interface will be essential to ensure that participants, including data subjects, can easily navigate the platform and exercise their rights. Simplicity in design will facilitate greater adoption and ensure that even non-technical users can engage effectively with the system, contributing to its overall success.

8. Integration with existing legal mechanisms

The platform will be designed to seamlessly integrate with existing legal mechanisms for data transfers, such as Binding Corporate Rules (BCRs), codes of conduct, and certification systems. By incorporating these established safeguards, the proposed system will enhance the legal enforceability of cross-border data transfers while offering an innovative and automated layer for dispute resolution. This integration ensures that the platform builds upon recognized legal frameworks, providing a robust and compliant solution for international data transfers.

9. Comparative analysis: smart contracts vs. traditional data transfer mechanisms

To evaluate the effectiveness of smart contracts in international data transfers, a comparative analysis was conducted between the proposed blockchain-based system and traditional procedural frameworks. The assessment focused

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

on five key dimensions: enforceability, compliance, efficiency, transparency, and dispute resolution.

Table 2. Comparative Analysis: Smart Contracts vs. Traditional Data Transfer Mechanisms

Criteria	Traditional Data Transfer Mechanisms (SCCs, BCRs)	Smart Contract-Based System
Enforceability	Requires manual enforcement through courts or regulatory authorities.	Self-executing and automated enforcement with supervisory authority oversight.
Compliance	Subject to jurisdictional discrepancies and evolving regulations.	Embedded compliance mechanisms aligned with GDPR SCCs and automated enforcement.
Efficiency	Time-consuming processes, often requiring extensive documentation and legal review.	Faster execution with predefined conditions, reducing administrative overhead.
Transparency	Limited visibility into contract execution and compliance status.	Immutable, auditable records stored on blockchain, ensuring full traceability.
Dispute Resolution	Requires legal proceedings, increasing costs and delays.	Hybrid model combining automated execution with authority-led arbitration.

Source: own elaboration.

The comparative analysis demonstrates that while smart contracts offer significant advantages in terms of automation, transparency, and efficiency, they require additional regulatory alignment to ensure enforceability across jurisdictions. By integrating supervisory authorities into the dispute resolution process, the proposed framework seeks to balance technological efficiency with legal safeguards, bridging the gap between existing data transfer mechanisms and blockchain-based automation.

VI. Results

This research presents a hybrid framework that bridges technological and legal dimensions to enhance data transfers while ensuring enforceable data subject rights and effective legal remedies. The proposed solution leverages smart contracts within a secure and interoperable platform, aimed at expediting dispute resolution and ensuring compliance with global data protection regulations.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

We began by analyzing the current state of international data transfers under the General Data Protection Regulation (Regulation (EU) 2016/679, 2016). Various transfer mechanisms were evaluated, including adequacy decisions, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), Codes of Conduct, Certification Mechanisms, Ad hoc Contractual Clauses, and International agreements. While these instruments provide legal pathways for cross-border data flows, they often face limitations in ensuring efficient enforcement and timely dispute resolution across multiple jurisdictions.

To address these challenges, the introduction of blockchain and Distributed Ledger Technology (DLT) as foundational infrastructures was proposed. These technologies provide immutable, transparent, and secure record-keeping systems, making them ideal for automating data transfers. Through the use of smart contracts, the platform automates the execution of data transfers based on approved SCCs or MCCs, thereby reducing the need for intermediaries and ensuring compliance with existing regulatory frameworks. Smart contracts facilitate self-executing agreements, offering transparency, accountability, and efficiency throughout the data transfer process.

Furthermore, the integration of supervisory authorities as escrow agents or guarantors within the platform was proposed to streamline dispute resolution. This mechanism allows supervisory bodies to oversee data transfers in real time, ensuring that legal obligations are met and providing a framework for the swift resolution of disputes. A key innovation of this system is the issuance of Non-Fungible Tokens (NFTs) to data subjects. These NFTs serve as unique digital triggers that enable data subjects to initiate complaints or activate dispute resolution processes in cases where their data protection rights are infringed. The use of NFTs ensures traceability, as each token is linked directly to the relevant transaction, thereby reinforcing accountability within the system.

To ensure compliance with data protection regulations and mitigate potential risks, a Data Protection Impact Assessment (DPIA) must be conducted before processing any personal data on the platform. This DPIA will assess the risks associated with data transfers and ensure adherence to GDPR and other global data protection standards. Supervisory authorities may also participate in the assessment to provide oversight and ensure compliance with legal frameworks.

In terms of security and privacy, the platform is designed with robust technical safeguards, including on-chain/off-chain configurations, encryption, hashing, and role-based access controls. These measures ensure that sensitive data is protected during transfers, while still allowing authorized entities to access the necessary information. The system employs on-chain storage for data

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

identifiers and off-chain storage for sensitive information to enhance privacy while maintaining transparency. Additionally, the platform incorporates legal documentation that clearly defines the rights, obligations, and roles of all participants, ensuring that the system operates within a transparent and legally sound framework.

An important consideration in the design of this platform is the use of tokens or cryptocurrencies to facilitate transactions. While the system can utilize a DLT-based network with cryptocurrency-based consensus mechanisms, we also explored an alternative model using a non-cryptocurrency consensus mechanism. This option may reduce regulatory and financial barriers in jurisdictions with stringent cryptocurrency regulations, offering a flexible yet secure method for data transfers.

Overall, the proposed platform offers an innovative and automated approach to resolving data protection disputes by integrating blockchain and smart contracts. This approach provides a faster, more efficient means of managing international data transfers while maintaining compliance with global data protection regulations. By enabling the direct involvement of supervisory authorities and data subjects, the platform strengthens accountability and empowers individuals to exercise control over their personal data in a secure and transparent manner.

Furthermore, the introduction of NFTs as triggers for exercising data subject rights marks a significant step toward greater informational self-determination. This model of sovereign identity empowers individuals to manage their digital identities autonomously, offering a new paradigm for digital governance in the context of cross-border data transfers.

In conclusion, this research demonstrates the potential of blockchain and smart contracts to revolutionize international data transfers, making them more secure, efficient, and transparent. Although the platform requires further technical development and regulatory approval, it represents a promising solution to the complex challenges posed by cross-border data transfers in the digital age. By harmonizing technological innovation with legal safeguards, this hybrid framework offers a forward-looking approach to data protection that aligns with the evolving needs of a globally connected world.

VII. Discussion

The introduction of this article provides a comprehensive analysis of the current challenges in international data transfers, with a focus on the GDPR as the primary global legal framework. It identifies three main mechanisms

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

for data transfers under the GDPR: adequacy decisions, appropriate safeguards, and derogations for specific situations. Additionally, the article highlights the challenges of complying with these mechanisms, particularly in the wake of the CJEU C-311/18 (Schrems II) decision, which invalidated the EU-U.S. Privacy Shield. This legal backdrop sets the stage for the proposed hybrid approach, which seeks to integrate advanced technological solutions, such as smart contracts, with established legal instruments to enhance data transfers and streamline dispute resolution processes.

In the Current State of Data Transfers section, the article provides a detailed examination of the various transfer mechanisms available under the GDPR, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), Codes of Conduct, Certification Mechanisms, Ad hoc contractual clauses, and International agreements/Administrative arrangements. It emphasizes the critical importance of conducting Transfer Impact Assessments (TIA) to ensure that data transfers comply with data protection laws and mitigate risks associated with cross-border data flows. The European Data Protection Board (EDPB) recommendations on how to conduct TIAs and facilitate compliance with transfer mechanisms are also discussed in detail.

The section Smart Contracts, Enforceable Data Subject Rights, and Effective Legal Remedies for Data Subjects introduces blockchain technology as the core infrastructure for the proposed solution. Blockchain is categorized into Public, Private, and Consortium models, with the article clarifying that blockchain networks typically process pseudonymized data, rather than anonymized data, which falls under the purview of data protection regulations. This clarification is crucial as it dispels the misconception that data on blockchain is fully anonymized and exempt from regulatory oversight. The article proposes that smart contracts self-executing contracts embedded in blockchain networks be utilized to automate the enforcement of Standard Contractual Clauses (SCCs) or Model Contract Clauses (MCCs). By automating these processes, smart contracts can enhance compliance with data protection regulations, reduce delays in data transfers, and provide a transparent and secure method for dispute resolution.

The integration of supervisory authorities as escrow agents or guarantors is another critical component of the proposed solution. This mechanism allows supervisory authorities to oversee data transfers in real time and to intervene in case of breaches or non-compliance. Furthermore, data subjects are empowered to exercise their rights through the issuance of Non-Fungible Tokens (NFTs), which act as unique digital triggers for initiating complaints or activating dispute resolution mechanisms. This system ensures that data subjects retain control over their personal data, providing an efficient and secure method

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

for enforcing their rights under data protection regulations. The use of NFTs also introduces a new layer of accountability, as each token is linked to a specific data transfer, allowing for traceability and transparency.

The Discussion section presents a well-reasoned argument for the integration of blockchain and smart contracts into the current data transfer framework. The hybrid approach combines established legal mechanisms with cutting-edge technology, offering a more efficient, secure, and transparent system for managing cross-border data flows. By leveraging blockchain's immutability and transparency, the proposed solution addresses many of the shortcomings of traditional data transfer mechanisms, such as the difficulty in ensuring compliance across jurisdictions and the complexity of resolving disputes in a timely manner.

In conclusion, the article demonstrates the potential of smart contracts and blockchain technology to revolutionize data transfers, offering a practical and scalable solution to the challenges posed by international data protection laws. While the proposed platform requires further technical development and regulatory approval, it represents a promising step toward a future in which data subjects can exercise greater control over their personal data, and data transfers can be managed more efficiently and securely. The integration of legal safeguards and technological innovation marks a significant advancement in the evolution of data protection frameworks, providing a forward-thinking solution to the complexities of data governance in the digital age.

VIII. Conclusions

The mechanisms for data transfers based on adequacy decisions provide an important foundation, but they often lack agility, interoperability, and scalability, making them difficult to execute effectively in many circumstances. To address these challenges, this article proposes a technological solution that complements existing transfer instruments by integrating smart contracts into the data transfer process. This innovation introduces greater transparency and integrity, automating the resolution of disputes and ensuring compliance with data protection regulations through standardized and machine-readable smart legal contracts.

The proposed platform goes beyond simply enabling digital complaints. By incorporating blockchain or Distributed Ledger Technology (DLT), the system offers a more autonomous level of automation, allowing for the self-execution of Standard Contractual Clauses (SCCs) and Model Contract Clauses (MCCs). However, it is essential to recognize that using blockchain or DLT

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

for personal data transfers constitutes high-risk processing. Therefore, prior to launching the system, the Data Controller must conduct a comprehensive Data Protection Impact Assessment (DPIA), with potential oversight from supervisory authorities as required by applicable legal frameworks and global standards.

While the GDPR restricts the transfer of personal data outside the EEA to jurisdictions with adequate levels of protection or appropriate safeguards, managing data flows on a public blockchain network introduces additional complexities. In particular, controlling the flow of data in decentralized networks where miners operate globally is a significant challenge. To address this, the proposed solution recommends starting with a private blockchain network or DLT, which offers better control and transparency, before exploring alternative configurations.

A key feature of the proposed platform is the automated dispute resolution mechanism. Unlike traditional arbitration panels, the supervisory authorities responsible for data protection would play an active role in resolving disputes. This approach avoids the need for legislative adjustments in each jurisdiction and provides a more streamlined, realistic solution for cross-border data transfers.

Although blockchain technology and smart contracts are gaining recognition, not all users are familiar with these technologies. Therefore, the platform's user interface (frontend) should prioritize simplicity and ease of use, while the backend remains technologically complex to ensure secure and efficient operations.

The system also integrates cryptocurrencies and tokens to facilitate key actions, such as signing agreements or activating dispute resolution processes. However, to address concerns about the volatility and regulation of cryptocurrencies, the platform can alternatively operate on a DLT network with a non-cryptocurrency-based consensus mechanism.

Finally, the use of Non-Fungible Tokens (NFTs) for triggering dispute resolution offers an efficient and practical solution for data subjects, eliminating the need for manual agreement signatures and reducing user fatigue. The issuance of an NFT upon the signing of SCCs or MCCs allows data subjects to maintain control over their data transfers, providing a transparent and traceable method to initiate disputes.

This article concludes that smart contracts offer a viable solution for automating and enforcing data protection regulations, complementing existing legal frameworks like SCCs and BCRs. By integrating these technologies into a single, interoperable platform, data subjects gain greater control over their personal data, paving the way for the development of a sovereign identity

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

model that enables real informational self-determination. This system represents a significant step forward in the evolution of international data transfers and the protection of individual rights in the digital age.

IX. References

Anusha, R., Jayashree, J., Vijayashree, J., and Yousuff, M. (2024). Blockchain for transaction of large-scale clinical information. In R. Malviya and S. Sundram (Eds.), *Blockchain for Healthcare 4.0: Technology, Challenges, and Applications* (pp. 245-261). CRC Press.

Bacon, J., Michels, J. D., Millard, C. and Singh, J. (2017). Blockchain demystified. *Queen Mary University of London School of Law Legal Studies Research Paper*, (268), 1-53.

Bashir, I. (2020). *Mastering blockchain; a deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more* (3a Ed.). Packt Publishing.

Commission Nationale Informatique et Libertés [CNIL]. (2018). Blockchain solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

Cubillos Vélez, Á. (2017). La explotación de los datos personales por los gigantes de Internet. *Estudios en Derecho a la Información*, *2*(3), 27-55. https://doi.org/10.22201/iij.25940082e.2017.3.10823

EU Blockchain Observatory and Forum. (2022). *Smart Contracts*. Available at: https://blockchain-observatory.ec.europa.eu/publications/smart-contracts_en

Hernández González, A. B. (2018). Protección de datos personales en el sector privado de la salud. *Estudios en Derecho a la Información*, 3(5), 83-100. https://doi.org/10.22201/iij.25940082e.2018.5.12123

Llamas Covarrubias, J. Z. (2020). Transparencia y protección de datos personales en la cadena de bloques (blockchain). *Estudios en Derecho a la Información*, *6*(11), 27-63. https://doi.org/10.22201/iij.25940082e.2021.11.15299

Ocampo Muñoa, M. G. (2019). Nuevos desafíos para la protección de datos personales en México. La regulación de la tecnología blockchain. *Estudios en Derecho a la Información*, *4*(8), 3-20. https://doi.org/10.22201/iij.25940082e.2019.8.13881

e-ISSN: 2594-0082

DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Prusty, N. (2018). *Blockchain for enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features*. Packt Publishing.

Ramamurthy, B. (2020). *Blockchain in action*. Manning Publications.

Red Iberoamericana de Protección de Datos [REDIPD]. (2022). Implementation guide on model contract clauses for international personal data transfers (IPDT). https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-en.pdf

Tang, A. (2023). *Privacy in practice: establish and operationalize a Holistic Data Privacy Program*. CRC Press.

The Law Society. (2022). *Blockchain legal and regulatory guidance* (2a Ed.). https://prdsitecore93.azureedge.net/-/media/files/topics/research/blockchain-legal-and-regulatory-guidance---second-edition-v267.pdf?rev=1765bd124b0749f89caaa40a61fbeebb&hash=7149D5F0DE53AD39608D5BA6304E61F2

Tribunal De Justicia De La Unión Europea (CJEU), 2018, Asunto C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, recuperado de https://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=EN

Upadhyay, N. (2019). *UnBlock the Blockchain*. Springer.

Voss, J. (2021). Data protection issues for smart contracts. In M. Corrales Compagnucci, M. Fenwick and S. Wrbka (Eds.), *Smart contracts: technological, business and legal perspectives* (pp. 79-100). Hart Publishing.

World Economic Forum [WEF]. (2019). Inclusive deployment of blockchain for supply chains: Part 4: Protecting your data. https://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_for_Supply_Chains_Part_4_Report.pdf

World Economic Forum [WEF]. (2020). Redesigning trust: Blockchain deployment toolkit. https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf

Parlamento Europeo y Consejo de la Unión Europea, 2016, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), *Diario Oficial de la Unión Europea*, L119/1, recuperado de http://data.europa.eu/eli/reg/2016/679/oj

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Parlamento Europeo y Consejo de la Unión Europea, 2023, Reglamento (UE) 2023/1232 del Parlamento Europeo y del Consejo de 14 de junio de 2023 sobre normas armonizadas de acceso justo y uso de datos (Ley de Datos), *Diario Oficial de la Unión Europea*, L165/1, recuperado de http://data.europa.eu/eli/reg/2023/2854/oj

EDPB. (2018). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

EDPB. (2021). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

EDPB. (2020). Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

Ast, F. (2020, September 23). Secure your contract with Kleros dispute resolution. *Kleros*. https://blog.kleros.io/secure-your-contract-with-kleros

EDPB. (2021). Guidelines 04/2021 on codes of conduct as tools for transfers Version 2.0. https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

EDPB. (2022). Recommendations 1/2022 on the application for approval and on the elements and principles to be found in controller binding corporate rules (Art. 47 GDPR). https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplicationform_en.pdf

EDPB. (2023). Guidelines 07/2022 on certification as a tool for transfers Version 2.0. https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf

Lesaege, C., George W. and Ast, F. (2021). Long paper v2.0.2. *Kleros*. https://kleros.io/yellowpaper.pdf

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

X. Appendices[1]

Appendix 1. Legal Contract[2]:

CONTRACT FOR THE OPERATION AND MANAGEMENT OF THE CROSS-BORDER DATA TRANSFER PLATFORM

BETWEEN

[NAME OF EXPORTER], a legal entity duly incorporated under the laws of [EXPORTER'S COUNTRY], with its registered office at [ADDRESS OF EXPORTER] (hereinafter referred to as "Exporter").

[NAME OF IMPORTER], a legal entity duly incorporated under the laws of [IMPORTER'S COUNTRY], with its registered office at [ADDRESS OF IMPORTER] (hereinafter referred to as "Importer").

[NAME OF SUPERVISORY AUTHORITY], acting as the escrow account manager for the platform, with its registered office at [ADDRESS OF SUPERVISORY AUTHORITY] (hereinafter referred to as "Supervisory Authority").

[NAME OF DATA SUBJECT], a natural person with data protection rights under applicable laws (hereinafter referred to as "Data Subject").

RECITALS

WHEREAS the Supervisory Authority manages the data transfer platform that facilitates cross-border data transfers in compliance with applicable data protection laws, such as the GDPR;

WHEREAS Exporters and Importers must register and acquire signing rights to use the platform, and Data Subjects must register with permissions to lodge complaints in the event of a violation of their data protection rights;

---

[1] The author is not responsible for your use or implementation of these contracts (Appendix 1. Legal Contract and Appendix 2. Solidity Contract).

[2] Data Protection Compliance clause has been added for GDPR compliance. Limitation of Liability clause limits liability in cases of unforeseen circumstances. Amendment and Termination clause to allow the contract to be modified or ended by mutual consent.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

WHEREAS the platform offers templates of Standard Contractual Clauses (SCCs) and Model Contractual Clauses (MCCs) approved by competent authorities for use by the Exporters and Importers;

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the parties hereby agree as follows:

Article 1: Definitions

Data Transfer Platform: The secure and interoperable platform for executing cross-border data transfers under SCCs/MCCs.
Smart Contract: A self-executing contract where the terms of the agreement are written directly into code and govern the data transfer between Exporters and Importers.
NFT: A non-fungible token issued to the Data Subject as proof of the executed contract and a trigger for filing complaints.
Supervisory Authority: The competent authority that oversees compliance with applicable data protection regulations and acts as escrow.

Article 2: Obligations of the Parties

Exporters and Importers agree to use the platform and the approved SCCs/MCCs for all cross-border data transfers. The smart contract execution is mandatory for completing the transfer.
Data Subjects are entitled to use the platform to file complaints via the NFT mechanism if their rights are violated.
Supervisory Authority will act as escrow for the contract and ensure that all parties comply with their obligations under data protection laws.

Article 3: Smart Contract Execution

Upon selecting the appropriate SCCs/MCCs, the Exporter and Importer will execute the smart contract on the platform, under the supervision of the Supervisory Authority. An NFT will be issued to the Data Subject as proof of the contract.

Article 4: Complaint Mechanism

If the Data Subject believes their rights have been violated, they can trigger the complaint mechanism using the issued NFT. The complaint will be forwarded to the competent Supervisory Authority for investigation.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Article 5: Dispute Resolution

The Supervisory Authority will resolve complaints by determining whether the Exporter or Importer violated data protection regulations. The ruling shall have legal force in the relevant jurisdiction.

Article 6: Data Protection Compliance

All parties agree to comply with applicable data protection laws, including GDPR, and ensure that personal data is handled in compliance with the highest standards of privacy and security.

Article 7: Limitation of Liability

The parties agree that neither the Supervisory Authority nor the platform operator shall be held liable for damages resulting from unforeseen circumstances, such as security breaches or technological failures, except in cases of gross negligence or willful misconduct.

Article 8: Amendments and Termination

This agreement may be amended or terminated by mutual written consent of all parties. In the event of termination, the obligations related to data protection shall survive.

Article 9: Governing Law

This contract shall be governed by and construed in accordance with the laws of [JURISDICTION]. Disputes shall be resolved by the courts of [JURISDICTION].

Signed:

[Signature of Exporter]
[Signature of Importer]
[Signature of Supervisory Authority]
[Signature of Data Subject]

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Appendix 2. Solidity Contract[3]:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";

contract DataTransferPlatform is ERC721 {
    uint public nextTokenId;
    address public supervisoryAuthority;
    uint public complaintDeadline;
    mapping(address => bool) public exporters;
    mapping(address => bool) public importers;
    mapping(address => bool) public dataSubjects;
    mapping(address => uint) public nfts; // Mapping for issued NFTs
    mapping(address => bool) public complaints;

    event ContractSigned(address indexed exporter, address indexed importer, address indexed dataSubject, uint nftId);
    event ComplaintFiled(address indexed dataSubject, address indexed exporterOrImporter, uint nftId);
    event ComplaintResolved(address indexed dataSubject, address indexed rulingParty, bool rulingInFavor);

    modifier onlySupervisoryAuthority() {
        require(msg.sender == supervisoryAuthority, "Only the supervisory authority can perform this action.");
        _;
    }

    modifier onlyRegisteredExporter() {
```

[3] ERC-721 Standard: Used for NFT creation, ensuring compatibility with widely accepted standards. Complaint Mechanism: A well-defined process for handling complaints, with events emitted for tracking actions. Resolve Complaint: A function to allow the Supervisory Authority to resolve disputes.

The Solidity code work when deployed using a platform such as Remix IDE or a local blockchain environment like Truffle with Ganache. The code adheres to Solidity 0.8.x standards and imports the required ERC-721 token standard from OpenZeppelin, which is a widely used, reliable library for smart contracts.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

```
        require(exporters[msg.sender], "Only registered exporters can perform this
action.");
        _;
    }

    modifier onlyRegisteredImporter() {
        require(importers[msg.sender], "Only registered importers can perform this
action.");
        _;
    }

    modifier onlyRegisteredDataSubject() {
       require(dataSubjects[msg.sender], "Only registered data subjects can perform
this action.");
        _;
    }

    constructor() ERC721("DataTransferNFT", "DTN") {
        supervisoryAuthority = msg.sender;
        complaintDeadline = 30 days; // Complaints must be filed within 30 days
    }

   function registerExporter(address exporter) external onlySupervisoryAuthority {
        exporters[exporter] = true;
    }

    function registerImporter(address importer) external onlySupervisoryAuthor-
ity {
        importers[importer] = true;
    }

    function registerDataSubject(address dataSubject) external onlySupervisory-
Authority {
        dataSubjects[dataSubject] = true;
    }

   function signContract(address exporter, address importer, address dataSubject)
external onlySupervisoryAuthority {
        require(exporters[exporter], "Exporter must be registered.");
        require(importers[importer], "Importer must be registered.");
```


e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

```
        require(dataSubjects[dataSubject], "Data Subject must be registered.");

        uint nftId = nextTokenId;
        _safeMint(dataSubject, nftId); // Issue NFT to data subject
        nextTokenId++;

        nfts[dataSubject] = nftId;

        emit ContractSigned(exporter, importer, dataSubject, nftId);
    }

    function fileComplaint(uint nftId) external onlyRegisteredDataSubject {
        require(nfts[msg.sender] == nftId, "Invalid NFT.");
        require(block.timestamp <= nfts[msg.sender] + complaintDeadline, "Complaint period has expired.");

        complaints[msg.sender] = true;

        emit ComplaintFiled(msg.sender, address(this), nftId);
    }

    function resolveComplaint(address dataSubject, bool rulingInFavor) external onlySupervisoryAuthority {
        require(complaints[dataSubject], "No complaint found.");

        // Implement complaint resolution logic (ruling, compensation, etc.)
        complaints[dataSubject] = false;

        emit ComplaintResolved(dataSubject, msg.sender, rulingInFavor);
    }
}
```


e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.20.19623

Cómo citar

Sistema IIJ
Llamas Covarrubias, Jersain Zadamig, "Automating data transfer compliance and dispute resolution with smart contracts", *Estudios en Derecho a la Información*, México, vol. 10, núm. 20, julio-diciembre de 2025, pp. 39-77. https://doi.org/10.22201/iij.25940082e.2025.20.19623

APA
Llamas Covarrubias, J. Z. (2025). Automating data transfer compliance and dispute resolution with smart contracts. *Estudios en Derecho a la Información*, *10*(20), 39-77. https://doi.org/10.22201/iij.25940082e.2025.20.19623