

Social Entrepreneurship: Challenges, Risks, and Opportunities¹

M^a José Vañó Vañó²

Abstract: This article explores the role of technology, interoperability, and digital identity in promoting social entrepreneurship within a secure and inclusive framework. Social entrepreneurship, with its focus on social impact, often requires adaptable technological solutions to overcome operational challenges. The principles of technological neutrality and interoperability allow entrepreneurs to adopt appropriate tools regardless of infrastructure, thereby enhancing inclusivity and resilience. The article examines European and Spanish regulations, such as eIDAS, GDPR, and the Spanish Social Economy Strategy, which support secure data practices and integration within the EU. By fostering collaboration and ensuring data security, these technologies create a robust environment for social enterprises that align with social economy values, promote equitable and sustainable development, and provide strong protections for all users.

Introduction

This study adopts a qualitative methodology based on documentary and regulatory analysis, with the aim of examining the impact of interoperability, blockchain, and digital identity on social entrepreneurship from a legal perspective. The sources include the main European and international regulatory frameworks, such as the Artificial Intelligence Regulation and the Council of Europe Framework Convention on Artificial Intelligence, as well as relevant national legislation in Spain, such as Law 14/2013 and the Social Economy Strategy 2023-2027.

The analysis is divided into three stages:

1. Examination of fundamental legal principles: An analysis of the principles for the protection of fundamental rights in the use of technologies applied to the social sphere, based on standards such as the EU Charter of Fundamental Rights.
2. Regulatory impact on social entrepreneurship: An evaluation of the security and transparency requirements established by European AI and interoperability regulations for the implementation of technologies in social entrepreneurship, with a particular focus on digital identity management.
3. Assessment of legal risks: An examination of the potential legal risks and liabilities associated with the use of AI and blockchain, using the Framework Convention on AI and Human Rights and the General Data Protection Regulation (GDPR) as reference frameworks.

In our work, we pose the following question: How does the adoption of interoperable technologies, such as blockchain and digital identity systems, improve the efficiency, transparency, and reach of social entrepreneurship projects? This question reflects an interest in exploring how technology not only enhances the operational capacity of social entrepreneurs, but also helps to build networks of trust and collaboration in environments that have traditionally faced resource constraints and limited market access.

The research question also invites an examination of the legal and ethical aspects of digitalization within social entrepreneurship, particularly in the context of data protection, privacy, and fundamental rights. In this regard, the work explores how a robust interoperability framework not

¹ Research developed in the framework of Project TED2021-129787B-I00, funded by MCIN/AEI/10.13039/501100011033 and by the European Union "NextGenerationEU"/PRTR, called KEY SELF-CONSUMPTION COMMUNITIES IN ENERGY TRANSITION (POWERCOOP). PI M^a José Vañó Vañó and Project CIPROM/2022/26 "Present and future of the regulation of Cryptoassets in the EU [Legalcripto]".

² IUDESCOOP Researcher/University Professor. Department of Commercial Law "Manuel Broseta Pont". Faculty of Law. University of Valencia. Researcher at the Research Institute of Social Economy, cooperativism and entrepreneurship of the UV mjvanyo@uv.es

only improves the efficiency of social organizations, but also ensures the protection and security of the digital identities of beneficiaries and collaborators. This approach allows us to assess the ability of technology to generate lasting social benefits while maintaining strong legal protections that support both entrepreneurs and the communities they serve.

1. The importance of technology in social entrepreneurship

Social entrepreneurship focuses on creating business initiatives that go beyond economic viability and seek to have a positive social impact by addressing social, economic, or environmental problems through innovative and sustainable solutions. In contrast to traditional businesses, their primary goal is collective well-being, prioritizing community benefit over personal profit (Monzón & Vaño, 2020). As agents of change, social entrepreneurs drive development and inclusion in their communities, creating an economy grounded in equity, social justice, and participation. The digital divide disproportionately affects marginalized communities, exacerbating existing inequalities and limiting access to technological advances. For example, rural areas, underserved urban regions, and groups with lower levels of digital literacy often lack access to the infrastructure and training needed to adopt emerging technologies such as blockchain and AI. These disparities are particularly pronounced in social entrepreneurship, where resource constraints and technology gaps hinder the scalability and effectiveness of initiatives aimed at addressing social challenges. In addition, interoperability challenges—stemming from fragmented legal and technical systems—create barriers to collaboration and data sharing between organizations, further marginalizing these communities. Addressing these challenges requires tailored strategies, including investments in digital infrastructure, education, and simplified interoperability frameworks, to ensure that technology-driven solutions are accessible and inclusive for all stakeholders.

Technology plays a fundamental role in social entrepreneurship, expanding the reach and effectiveness of these projects. Technology tools, including interoperability functions and advanced data management systems make it possible to optimize resources, manage initiatives more efficiently and transparently, and protect sensitive data. These capabilities increase transparency, reduce the risk of misuse of funds, and strengthen the credibility of projects, allowing social entrepreneurs to build a solid support network involving donors, collaborators, and beneficiaries (Vaño & Audivet, 2023).

Interoperability is particularly valuable in the social domain, enabling organizations and stakeholders to collaborate effectively by integrating their platforms and ensuring secure, structured access to relevant information. This is especially important in contexts where public-private collaboration is essential for addressing high-impact social issues. In addition, interoperability facilitates ethical and shared data management, ensuring compliance with data protection regulations and the ethical standards of the social economy. A well-managed technology framework not only helps social initiatives meet legal and ethical standards, but also fosters accountability and trust, ultimately benefiting all stakeholders.

In Spain, regulatory support for social entrepreneurship in the technology sphere is reflected in various initiatives and laws. Law 14/2013, on support for entrepreneurs and their internationalization, facilitates access to financing and promotes digital tools to improve the competitiveness of social projects. For its part, the Spanish Social Economy Strategy 2023-2027 fosters social innovation, digitalization, and public-private collaboration to strengthen the sustainability and impact of these initiatives. It underscores the role of advanced technologies in improving the efficiency and global reach of social economy projects.

At the international level, the United Nations (UN) recognizes the importance of social entrepreneurship in achieving the Sustainable Development Goals (SDGs). In particular, SDG 8, which focuses on decent work and economic growth, highlights the need to promote entrepreneurship and innovation as drivers of sustainable development, while SDG 9 promotes the use of advanced technological infrastructure for inclusive development. Agencies such as the

United Nations Development Programme (UNDP) and the United Nations Conference on Trade and Development (UNCTAD) support social entrepreneurship projects through funding, technical advice, and access to global networks. The Sustainable Development Solutions Network (SDSN) facilitates access to knowledge, resources, and collaborative networks and promotes partnerships between governments, businesses, and civil society organizations to develop technological solutions that contribute to achieving the SDGs.

Technology not only optimizes the processes of social entrepreneurship, but also contributes to building an ecosystem where data is protected, and the active participation of beneficiaries is encouraged. Interoperability and technological neutrality allow social entrepreneurs to adopt effective and accessible solutions without being limited by technological barriers, thereby promoting equitable and resilient development in their communities (Vaño & Audivet, 2023). In this way, technology becomes a catalyst that expands the capacity of entrepreneurs to act, reinforces the values and goals of social entrepreneurship, and directs initiatives toward the continuous improvement of living conditions and inclusive and sustainable development.

Social entrepreneurship faces specific technological challenges that limit its impact and sustainability. The digital divide remains a critical barrier, leaving many vulnerable communities without access to basic technologies. In addition, the implementation of advanced solutions such as blockchain or AI faces financial and technical obstacles, particularly in less developed regions. The lack of interoperability between technological systems exacerbates these problems and hinders collaboration between NGOs, governments, and the business community. Finally, digital exclusion threatens to marginalize groups such as the elderly and rural communities, further deepening existing inequalities. These barriers highlight the need for inclusive regulatory strategies, such as the Artificial Intelligence Act (the AI Act) and the Spanish Social Economy Strategy, to ensure that these technologies are accessible and equitable.

Technology provides powerful tools to enhance the impact of social enterprises, as demonstrated by practical applications of blockchain and AI. For example, platforms such as Giveth leverage blockchain³ to increase transparency in donation tracking, allowing donors to monitor the allocation and use of their contributions in real-time, thereby building trust among stakeholders. Similarly, organizations such as Feeding America⁴ are using AI to optimize the distribution of food resources, using real-time data to match surplus supplies with areas of greatest need, reducing waste and increasing efficiency. These examples highlight how the adoption of cutting-edge technology can help social enterprises achieve greater scalability, transparency, and operational success.

Gstrein et al. (2024) emphasize that the governance of general-purpose AI (GPAI) under the AI Act presents unique challenges due to its broad applicability and systemic risks. They argue that while the AI Act aims to establish a high standard for AI regulation, it must balance innovation with democratic legitimacy and accountability, particularly in addressing the unforeseen consequences of GPAI in social and economic contexts. This highlights the need for a more adaptive and inclusive regulatory approach to address the diverse implications of AI technologies in the context of social entrepreneurship.

2. Challenges of technologically interoperable identity

The interoperability of digital identity systems is a major challenge for social entrepreneurs, who must ensure the security and privacy of personal data in an environment where trust is paramount. The interoperable management of digital identities makes it possible to integrate platforms and services with both public and private systems, facilitating access to essential services without compromising data protection (Vaño, 2021). This approach, grounded in technological neutrality and compliance with European data protection regulations, responds to the need to create inclusive

³ <https://giveth.io/es/landings/refi>

⁴ <https://www.feedingamerica.org/>

and accessible digital environments that ensure the equal participation of all actors in social entrepreneurship (Vaño et al., 2022).

Interoperability is a critical enabler for cross-border collaboration in social entrepreneurship, yet it often faces significant challenges due to the lack of universally applicable standards. Frameworks such as eIDAS and the AI Act provide important guidelines for harmonizing technological and legal systems within the European Union. However, their implementation can also complicate collaborations in transnational contexts. For example, while eIDAS promotes the seamless integration of digital identities across member states, disparities in infrastructure and digital readiness between countries may hinder its adoption, particularly in resource-constrained regions. Similarly, the AI Act's focus on high-risk applications ensures robust governance, but may inadvertently impose financial and technical burdens on smaller social enterprises, limiting their ability to innovate or expand internationally. Addressing these issues requires not only refining existing frameworks, but also promoting capacity-building initiatives to ensure that all stakeholders can fully engage with interoperable systems. Examples of technologies being applied for these purposes include blockchain-based smart contracts, which can automate data protection agreements and policies. This eliminates the need for intermediaries and allows social entrepreneurs to focus on their goals without taking on additional risk. Furthermore, in the context of local government, municipalities can use reserved contracts to award social services to social economy enterprises, fostering an inclusive and sustainable environment.

The concepts of AI,⁵ interoperability, smart contracts, and blockchain have become integral to our daily work, permeating all levels of activity across both the public and private sectors, as well as the broader economic landscape.⁶ The post-pandemic era has significantly accelerated technological development, introducing new concepts into our vocabulary at an unprecedented rate. We find ourselves in the age of the Internet of Things and process automation, standing at the threshold of the so-called Industry 4.0. This period marks a profound transformation in the use of information and communication technologies, with society—propelled by the recent global health crisis—adapting continuously to rapid technological change.⁷

In the digital age, the efficient and secure management of digital identities is essential to ensure the protection of personal data and the operational resilience of systems. In this context, the eIDAS GDPR⁸ in the European Union play essential roles in ensuring security and operational control.

The revision of the eIDAS Regulation (2014),⁹ culminating in the European Digital Identity Regulation (2024),¹⁰ represents a pivotal step in the digital transformation of the European Union. By introducing a unified and secure digital wallet, this framework aims to provide citizens with unprecedented control over their personal data and facilitate seamless access to public and private services. While the initiative reflects the EU's commitment to enhancing interoperability and data protection—in line with GDPR standards—it also poses significant challenges that must be critically addressed. The harmonization of technical and legal systems across member states remains a complex task, requiring significant collaboration and investment. In addition to aligning their infrastructure, member states must also address disparities in digital literacy and access, which

⁵ European Commission: Artificial Intelligence for Europe {SWD (2018) 137 final}, COM(2018) 237 final. Brussels, 25 April 2018, p. 2

⁶ López Jiménez D (2019) 79-119. Merchán Murillo A (2019) 50

⁷ https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1685

⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) <http://data.europa.eu/eli/reg/2016/679/oj>

⁹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02014R0910-20140917>

¹⁰ Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European digital identity framework <http://data.europa.eu/eli/reg/2024/1183/oj>

risk exacerbating existing inequalities. Furthermore, the regulation's emphasis on interoperability and security introduces potential tensions between ensuring accessibility for all users and maintaining robust safeguards against misuse or breaches.

These challenges underscore the importance of moving beyond technical compliance to ensure the practical usability and inclusivity of the system. For example, while the regulation sets a high benchmark for data protection, its implementation requires significant financial and technological resources, which may be a burden for less digitally advanced member states. In addition, public trust is paramount to adoption, requiring transparency in how personal data is managed and a clear communication strategy to address potential concerns about privacy and security. Without addressing these issues, the promise of a unified European digital identity may not be fully materialized, leaving vulnerable groups behind and limiting the transformative potential of this ambitious project.

While existing regulations, such as the AI Act and blockchain-specific frameworks, aim to promote the ethical use of technology, they often fall short in addressing the unique needs of social enterprises. For example, compliance requirements for blockchain systems can impose prohibitive costs on small NGOs, limiting their ability to adopt these technologies. Similarly, the AI Act, while robust in terms of risk mitigation, places significant emphasis on transparency and accountability measures that may be challenging for resource-constrained social enterprises to meet. These gaps highlight the need for tailored regulatory solutions that balance innovation with the practical realities of organizations operating in the social economy.

The updated digital identity framework addresses the limitations of the previous version of eIDAS and extends its scope beyond public services to include private transactions. Under this framework, the introduction of European digital identity wallets will enable EU citizens and residents to securely manage their digital identity in a unified system, providing them with exclusive control over their personal data.

The eIDAS reform incorporates key principles of the GDPR, ensuring that all data processing activities within the framework meet high standards of privacy and security. This includes important measures such as data minimization and purpose limitation, which are essential at a time when data privacy is a growing public concern.

Closely aligned with GDPR principles, the revised eIDAS framework mandates that data processing within the digital identity system respects privacy rights. The regulation emphasizes the collection of only necessary data for specified purposes and provides EU citizens with comprehensive control over their personal data through digital identity wallets. These wallets allow users to manage, view, and control data sharing, with security built in by design and default, including encryption and authentication to protect against unauthorized access. Additional safeguards prevent data amalgamation by identity providers, while users can track, audit, and request deletion of data as needed. The framework enhances interoperability, enabling secure identification across member states while introducing measures to prevent identity misuse.

International frameworks provide important guidance for ensuring the ethical and effective use of technology in social entrepreneurship. The Council of Europe's Framework Convention on Artificial Intelligence emphasizes the need for AI systems to respect human rights, democracy, and the rule of law, offering critical safeguards against potential misuse. Similarly, the United Nations Convention on Electronic Communications promotes principles such as technological neutrality and cross-border recognition of electronic documents, which are essential for advancing interoperability in global social initiatives. These frameworks align with existing EU regulations, such as eIDAS, to create a cohesive legal environment that supports both innovation and inclusivity in the social sector.

While technologies such as artificial intelligence and blockchain offer significant potential for social entrepreneurship, they also pose notable risks that can disproportionately affect vulnerable communities. Algorithmic discrimination in AI-based solutions poses a serious threat, as biased data or poorly designed algorithms can exclude or harm marginalized groups. Blockchain, despite its promise of transparency, faces scalability challenges and high initial implementation costs, making it less accessible to resource-constrained social enterprises. Furthermore, ethical concerns related to the management of personal data—such as privacy breaches or misuse—are particularly critical in the social sector, where protecting sensitive information about beneficiaries is essential. Addressing these risks requires robust regulatory frameworks and tailored safeguards to ensure that these technologies are deployed ethically and inclusively, and to avoid unintended consequences that could deepen existing inequalities.

A critical issue in the regulation of AI is its potential to perpetuate existing social biases, including gender inequality. Senent Vidal & Ventura Franch (2024) emphasize that without explicit safeguards, AI systems risk reinforcing discriminatory patterns embedded in training data and algorithmic design. For example, they highlight the risk of "black box algorithms," which operate without transparency, making it difficult to trace or mitigate discriminatory outcomes. While the AI Act introduces measures to limit high-risk applications, the authors argue that it falls short of addressing gender-specific biases in a systematic and comprehensive way.

In addition, the authors propose that the regulation mandate gender equality and non-discrimination training for both AI developers and users. They also advocate for gender balance in decision-making bodies related to AI governance, emphasizing that inclusive representation fosters diverse perspectives and helps mitigate bias at its root. While acknowledging progress—such as European Parliament amendments addressing algorithmic discrimination—they criticize the AI Act's fragmented approach and call for a more integrated, cross-cutting application of gender perspectives across all regulatory provisions.

The integration of advanced technologies like Big Data is transforming the way social enterprises tackle complex societal challenges. By enabling real-time processing and analysis of large datasets, Big Data presents unique opportunities to optimize resource allocation, predict community needs, and assess the impact of social initiatives. However, its conceptual ambiguity complicates its adoption. Han, Gstrein & Andrikopoulos (2024) note that while the "V" characteristics—volume, velocity, and variety—are widely acknowledged, there is no consensus on a single definition of Big Data. This lack of clarity hinders interdisciplinary collaboration and the development of tailored applications in the social sector. Without clear standards, social enterprises risk misapplying the technology or underestimating its potential to address pressing issues such as poverty alleviation, education, and public health. Establishing a shared understanding of Big Data and its practical implications is therefore essential to unlocking its transformative potential in social entrepreneurship.

3. Democratizing technology through interoperability and technological neutrality

Interoperability and technological neutrality are fundamental to democratizing access to technology in social entrepreneurship. These principles enable social entrepreneurs to implement solutions that adhere to open standards, ensuring fair access to digital services regardless of technological infrastructure or resources (Gendler, 2015). Network neutrality regulation and interoperability between systems ensure that all participants in the social entrepreneurship ecosystem can collaborate without technological barriers, fostering an inclusive environment where the benefits of digitization are accessible to all (Belli & De Filippi, 2016).

Interoperability allows diverse technological systems to communicate and exchange information efficiently, facilitating collaboration between social enterprises, public entities, and private partners. This connectivity enables frictionless data flow, resource sharing, and coordinated actions

across sectors, significantly enhancing the capacity of social enterprises to operate within inclusive and collaborative networks (Meira and Vañó, 2022).

Technological neutrality enhances interoperability by allowing social entrepreneurs to adopt appropriate technologies without being restricted to specific providers or platforms, ensuring equal access to digital tools regardless of technological infrastructure (Vargas Vasserot, 2022). In sectors such as energy, interoperability and neutrality have enabled cooperatives to engage in community initiatives, fostering sustainable energy access for marginalized communities through adaptable regulatory frameworks (Meira & Vañó, 2024).

These principles amplify the social impact of technology by ensuring adaptable, inclusive solutions aligned with social economy values such as transparency, participation, and collective benefit. Neutral and interoperable technologies help social enterprises bridge digital access divides, ensuring underserved populations benefit from technological advancements while enhancing project resilience and sustainability in pursuit of social equity and sustainable development.

Cybersecurity and data protection regulations have evolved to meet the demands of e-government and technological advances. A key principle in this context is net neutrality, introduced by Tim Wu in 2003, which requires equal treatment of all Internet content and prevents Internet service providers (ISPs) from restricting access to content (Gendler, 2015). Net neutrality preserves the Internet's open architecture, as noted by the Internet Society in 2016,¹¹ and is essential for barrier-free trade, lower transaction costs, and the protection of human rights and competition (Belli & De Filippi, 2016). Beyond the economic benefits, net neutrality safeguards fundamental rights, including freedom of expression and fair commercial activity (Robles Carrillo, 2019).

Net neutrality ensures four key user freedoms: connecting devices, running applications, accessing desired content, and receiving transparent information about service plans. However, challenges such as application blocking, ISP monopolization, and service prioritization must be addressed to maintain a fair and open digital environment.¹² Without net neutrality, ISPs could manipulate the flow of data, jeopardizing quality of service, digital fairness, and unrestricted access to online content.¹³

The regulation of net neutrality in Europe represents a cornerstone in the protection of fundamental rights such as democracy, the rule of law, and equal access to information. Regulation (EU) 2015/2120, often referred to as the Internet Neutrality Regulation or the Telecoms Single Market Regulation, enshrines the principle of non-discriminatory traffic management and prohibits ISPs from blocking, throttling, or prioritizing traffic for commercial gain. While these measures promote fairness and transparency, they also raise questions about their long-term sustainability and the practical challenges of enforcement. The allowance of "specialized services," such as telemedicine or high-quality streaming, reflects the flexibility of the regulation to accommodate emerging technologies. However, this flexibility also creates potential risks of undermining the open Internet if these services are not carefully monitored to ensure that they do not degrade the quality of general access.

From an operational perspective, the enforcement mechanisms delegated to National Regulatory Authorities (NRAs) under the guidance of BEREC¹⁴ provide a robust framework for oversight and transparency. However, the complexity of overseeing compliance across diverse markets highlights the differences in regulatory capacity among member states. This uneven enforcement can lead to fragmented user experiences and raise questions about the ability of regulation to ensure equitable outcomes across the EU. For example, while NRAs are tasked with publishing annual reports and

¹¹ <https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-NetworkNeutrality-20151030-es.pdf>

¹² Wu T (2003)

¹³ Matter F (2016) 95-98. Wu T (2003) 141

¹⁴ <https://www.berec.europa.eu/en>

ensuring adherence to the principles of net neutrality, their ability to address rapidly evolving digital landscapes and ISP practices remains limited by resources and jurisdictional constraints.

The EU's emphasis on technological neutrality through regulations such as 2015/2120 underscores its commitment to fostering an open and innovative digital ecosystem. However, this principle must contend with emerging challenges, such as ensuring fair competition among ISPs while integrating advanced services that require guaranteed quality of service. The balance between allowing innovation and safeguarding user rights is delicate, particularly as technologies such as 5G and edge computing gain prominence. Without continuous updates to adapt to these technological advancements, the regulation risks becoming obsolete in addressing new forms of digital inequality.

Closely related to net neutrality is the concept of interoperability, which has evolved from a technical to a legal framework. Interoperability between systems enables cross-border services and harmonizes the protection of rights through compatible regulations (Vañó, 2021). This is particularly relevant in e-commerce and international trade, where regulatory alignment prevents artificial barriers imposed by ISPs. By ensuring non-discriminatory data treatment, net neutrality and interoperability work together to promote an inclusive, transparent, and legally harmonized digital ecosystem.

Interoperability, as a complementary pillar of the EU's digital strategy, has been championed through initiatives such as IDABC, ISA, and now the Digital Europe Program. While these programs aim to harmonize technical and regulatory systems, their implementation often faces significant hurdles. The need for substantial investment in infrastructure and digital literacy to bridge the gaps among member states remains critical. Similarly, the ambitious goals of the Digital Single Market and Regulation (EU) 2015/2120 hinge on collaborative efforts between governments, businesses, and civil society to align diverse systems and policies. However, the persistent gap in digital readiness across the EU underscores the challenge of achieving a truly unified digital environment.

At the national level, Spain's General Telecommunications Law 11/2022 reinforces these principles by enshrining net neutrality as a fundamental right. However, its effectiveness depends on rigorous enforcement, particularly through the mechanisms established under Article 76. The Ministry of Economic Affairs and Digital Transformation and the National Cryptologic Center play pivotal roles in aligning national regulations with EU objectives, but these efforts must overcome systemic inefficiencies and limited resources to fully realize their potential.

The revised eIDAS framework enhances interoperability by enabling secure communication between electronic identification systems across member states. Through common standards and protocols, it facilitates cross-border access to public and private services, fostering digital inclusion and seamless interaction in areas such as healthcare and public administration.

Interoperability is essential for the development of digital services, enabling greater mobility in the areas of employment, education, and tourism by allowing unrestricted use of digital services. It also strengthens the digital single market, as interoperability—alongside security—drives trade and investment across the European Union, fostering economic growth. Moreover, interoperability enhances security and user trust, as interoperable systems are designed with high security standards, ensuring that digital identities remain resilient against fraud and cyber-attacks.

The period established by the Single Transitional Provision of Royal Decree 311/2022 of May 3, 2002, which regulated the National Security Scheme (ENS) for information systems in the public and private sectors, with the aim of providing security for the interconnection of information systems, giving them maximum security, has recently expired. The main objectives of the ENS were to increase confidence in the ability of information systems to adequately provide their services and to protect information without interruption or uncontrolled modification; to prevent information from reaching unauthorized persons; and to establish security measures for systems,

data, communications, and electronic services to facilitate citizens and public administrations in the exercise of their rights and the fulfillment of their obligations.

Royal Decree 203/2021 strengthens ENS compliance in the electronic operations of the public sector, while Organic Laws 3/2018 and 7/2021 emphasize the implementation of ENS measures for the protection of personal data. The cybersecurity strategy, supported by Royal Decrees 1008/2017 and 1150/2021, identifies cyberspace as a critical area requiring robust regulation. Additional legislation, such as Royal Decree 951/2015 and Regulation (EU) No. 910/2014 (eIDAS), updates the ENS to current cybersecurity needs.

This legal framework, together with the National Cybersecurity Strategy 2019 and the National Cybersecurity Plan 2022, emphasizes a coordinated approach to cyber threats and ensures a secure digital environment. Both Spanish and European regulations establish criteria for security and standardization to ensure interoperability in public administrations,¹⁵ including the use of XML standards for secure document tracking.¹⁶

Interoperability regulations cover electronic documents, digitalization, electronic files, signature policies, and data management, with the goal of unifying standards across public and private entities at all levels (Vaño, 2012). Following UN "best practices" for fraud prevention, organizations are encouraged to adopt reputable methods to detect and prevent commercial fraud, with strict adherence by companies and employees.¹⁷

In summary, while the EU's regulatory framework for net neutrality and interoperability represents a significant achievement, it needs to be continuously adapted to the evolving digital landscape. The challenge is not only to maintain fair and open access to Internet services, but also to ensure that these regulations do not inadvertently exacerbate existing inequalities. A critical and forward-looking approach is essential to ensure that these frameworks remain robust, equitable, and fit for purpose in a rapidly changing technological environment.

4. International goal: be interoperable and technologically neutral

In the context of international policy cooperation for procurement interoperability, it is crucial to understand how global stakeholders are working together to create regulatory and technical frameworks for cross-border electronic transactions. Key international bodies, such as the United Nations Commission on International Trade Law (UNCITRAL), play a central role in establishing standards that support interoperability. For example, UNCITRAL has developed frameworks such as the Model Law on Electronic Commerce and the Guide on the Implementation of Digital Signatures, aimed at harmonizing regulations and facilitating international e-commerce and contracting.¹⁸

Contracting and interoperability in the digital domain are vital for global business and technology interactions. As transactions become more automated, the need for interoperable systems across legal and technological jurisdictions increases. International cooperation, led by organizations such

¹⁵ Law 11/2007, of June 22, 2007, on citizens' electronic access to Public Services. Currently reformulated through the Resolution of June 28, 2012, of the Secretary of State for Public Administrations, which approves the Technical Interoperability Standard for the Relation of Data Models (BOE of July 26).

¹⁶ The ENI is aligned with the European Interoperability Strategy http://administracionelectronica.gob.es/pae/Home/dms/pae/Home/documentos/Estrategias/pae/Interoperabilidad_Inicio/isa_annex_i_eis_en/%20Estrategia%20Europea%20de%20Interoperabilidad.pdf and the European Interoperability Framework http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf. See in this regard the initiatives carried out by the XBRL Spain organization in which public bodies such as the Bank of Spain, National Securities Market Commission, Mercantile Registrars of Spain, Ministry of Economy and Public Administrations, or the National Institute of Statistics, as well as Universities and private companies participate. Vaño (2015) 185-198

¹⁷ http://www.uncitral.org/uncitral/es/uncitral_texts/payments/2013-indicators-of-commercial-fraud.html

¹⁸ UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001) (United Nations publication, Sales No. E.02.V.8), par. 107, and UNCITRAL Model Law on Electronic Transmittable Documents (United Nations publication (2017)), par. 122. Ávila Gonzales, NP (2023).

as UNCITRAL, is essential to create frameworks for automated contracting that ensure legal validity across borders. UNCITRAL emphasizes technological neutrality, ensuring the validity of contracts regardless of the method used.

Efforts focus on making contracts internationally interoperable, which requires harmonized regulations, data formats, security protocols, and privacy practices. Policy cooperation addresses jurisdictional issues in cross-border transactions.

Information exchange with legal content must be secure, protecting both the media and transmission networks. Technologically biased regulations can hinder market development by excluding unrecognized technologies, thereby compromising legislative efficiency and market freedom.

Numerous legal regulations control the circulation of data content, including the Organic Law 3/2018 on data protection and electronic signature regulations, Law 39/2015 on administrative procedures, and Royal Decree 1496/2003 on electronic invoicing. Blockchain, used alongside XML, enhances data structuring with a focus on privacy and security (e.g. GDPR) (Vaño 2005, 2008).¹⁹ It enables "sovereign identity" (SSI), giving users full control over their network information. Blockchain's design prevents post-publication changes and secures processes with dual electronic signatures and timestamps, creating "smart documents." As blockchain networks and smart contracts evolve, oversight roles will be automated, with the integrity of the document being verified by its hash rather than the document itself being stored on the blockchain.

The *"Report with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets (2020/2034(INL))"*²⁰ makes several requests. Notably, it emphasizes the need for a pan-European taxonomy for new products like crypto-assets to facilitate collaboration between different jurisdictions and provide greater legal certainty for market participants.

It is essential to establish a legal framework for crypto-assets to ensure proper monitoring and supervision by public authorities. A unified regulatory approach across the European Union is necessary to avoid unilateral measures that could lead to market fragmentation, legal uncertainty, and uneven competition. All participants in crypto-asset activities must adhere to rules on consumer protection, anti-money laundering, and market integrity, equivalent to those in Directive 2014/65/EU (MiFID 2).²¹ This will prevent the legitimization of crypto-assets used in illicit activities, safeguarding consumers and market stability.²²

This technology also guarantees a high level of traceability and security in online economic transactions. It is a system based on trust, an authorized registry trusted by everyone within the network (there is no central authority), verification of each transaction as it arrives at each node and before it propagates to the other nodes in the network, validation of transactions in new blocks through data mining, validation of the blocks generated by all nodes, and the addition of the newly generated blocks to the chain with the greatest computational effort.²³

¹⁹ Law 59/2003 of December 19 on Electronic Signatures, repealed by Law 6/2020 of November 11, regulating certain aspects of electronic trust services, provides us with the concept of electronic document that will enable us to give meaning to the interoperability, security and integrity pursued by the National Interoperability Scheme (ENI).

²⁰ https://www.europarl.europa.eu/doceo/document/A-9-2020-0161_EN.html

²¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065>

²² In Europe, the standardization of Distributed Ledger Technologies (DLT) and Blockchain is advancing, particularly through ISO/TR 24878. This initiative highlights best practices and trends, such as Web 3 and tokenization, to guide decision-makers on new business opportunities and technical advancements.

²³ EUROPEAN COMMISSION: Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee: A balanced system of intellectual property enforcement in response to today's societal challenges COM/2017/0707 final, November 29, 2017.

UNCITRAL's *Draft Provisions on Automated Contracting*²⁴ emphasize technological neutrality and non-discrimination, ensuring that digital contracts are valid regardless of their technological form. This requires a legal framework that supports interoperability across systems while complying with local and international regulations. The UNCITRAL Working Group is updating terminology to align with current technologies, recommending terms such as "data message processing" and "legal effectiveness" to ensure clarity and neutrality.

Automated contracting is transforming international e-commerce, necessitating common standards for secure cross-border transactions. Regulation (EU) 2015/2120 and UNCITRAL's draft provisions emphasize equal treatment of digital and traditional contracts, with providers required to meet legal requirements for contract formation, data protection, and privacy. However, automated procurement faces oversight and compliance challenges that require collaboration between national regulators and international bodies to establish fair and interoperable systems.

Interoperability poses unique challenges in the context of social entrepreneurship—particularly due to the lack of universal standards tailored to the needs of the social sector—a situation that hinders the seamless integration of technology systems across NGOs, governments, and private entities that often need to work together to address complex social issues. This fragmentation limits the efficiency and scalability of social initiatives and creates barriers to the effective use of shared data and resources. In addition, technical and regulatory disparities between platforms exacerbate these difficulties, particularly in cross-border or resource-constrained environments. To address these issues, frameworks such as eIDAS and the AI Act provide valuable guidance for building secure, interoperable systems that promote collaboration and inclusion in the social sector.

5. Technological and legal interoperability

Technological and legal interoperability is crucial for social entrepreneurs to be able to operate in a secure and reliable digital environment. Through the use of standards such as XML and blockchain, social entrepreneurship can facilitate the exchange of information in a structured and validated manner, ensuring data integrity and transparency in operations (Vaño, 2015). The implementation of technologies compatible with international legal frameworks, such as those developed by UNCITRAL, makes it possible to harmonize practices and regulations, thus facilitating cross-border collaboration, which is essential in the context of projects with global social impact (UNCITRAL, 2020).

Although UNCITRAL serves as the basic system of legal harmonization in the field of commercial law, it is equally true that since the 1990s, numerous global initiatives have successfully promoted interoperability and adapted to technological advancements in order to bridge the so-called digital divide.

For Internet transactions to be truly secure, various mechanisms must ensure authentication, confidentiality, transactional integrity, non-repudiation, and timestamping. Achieving this requires an alignment of technological and legal measures. Only through the proper integration of robust technological solutions with a sound legal framework can electronic transactions be truly secure and reliable.

Technological measures include protocols, interoperability schemes, and unique computer languages such as eXtensible Markup Language (XML) and blockchain, among others (Vaño 2015). In parallel, legal tools aim to establish standards that define basic parameters and essential requirements to be upheld in any legal relationship formalized through the network.

²⁴ United Nations Commission on International Trade Law Working Group IV (Electronic Commerce) 66th session Vienna, 16-20 October 2023. *Draft provisions on automated contracting* https://docs.un.org/en/A/CN.9/WG.IV/WP.182_v2306387.pdf (un.org)

XML is configured as a facilitator for the exchange of legal information from a dual perspective: the contractual one and the one related to the exchange of information between public bodies.²⁵ With regard to the first perspective, this language allows contracts to be pre-defined by the parties and validated at the time of their creation, thus avoiding subsequent modifications that are neither desired nor negotiated by the contracting parties. Structured and constantly updated databases are created in real time. While technologies such as XML play a key role in the management and protection of information in electronic transactions (Vaño 2015), a major drawback is the multicultural diversity of legal systems and languages, which may delay the use and implementation of such technologies.

While initially seen as a technical element, interoperability now requires the coordination of schemas and taxonomies, guided by regulatory standards. These frameworks have influenced national interoperability strategies across the EU. Programs such as ISA² continue to promote interoperability solutions for European public administrations, businesses, and citizens.

The main objective of ISA² is to improve the efficiency and effectiveness of public administrations by promoting interoperability, which contributes to the quality of public services and facilitates collaboration and information exchange between different agencies and countries. In addition, by harmonizing administrative and technical procedures, ISA² makes it easier for companies to operate in multiple EU countries and for citizens to move freely without facing bureaucratic obstacles.

The program also supports the effective implementation of EU policies by developing interoperable solutions that can be reused in various contexts. In this sense, ISA² encompasses several dimensions of interoperability: technical, semantic, organizational, and legal. Technical interoperability focuses on the development and promotion of standards that enable different systems and applications to work together efficiently. Semantic interoperability ensures that shared information is understood uniformly, regardless of the origin of the system. Organizational interoperability facilitates cooperation and coordination between different organizations and public administrations. Finally, legal interoperability focuses on aligning legal and regulatory frameworks to support the other forms of interoperability.

6. Final notes

The use of interoperable technologies in social entrepreneurship has the potential to revolutionize the way social impact is achieved, but it also poses significant ethical and practical challenges. While these technologies promise to increase inclusion, transparency, and efficiency, their implementation often reinforces pre-existing inequalities. The digital divide, a persistent barrier for marginalized communities, remains largely unaddressed in many regulatory frameworks. Without targeted interventions to expand digital literacy and infrastructure, these technologies risk becoming tools that primarily benefit resource-rich stakeholders, leaving behind the very populations they aim to empower.

Furthermore, the reliance on frameworks such as eIDAS and the AI Act to guide interoperability and digital identity raises questions about their accessibility and equity. These regulations, while ambitious, place a disproportionate burden on smaller social enterprises that may lack the technical and financial capacity to comply. For example, the high cost of implementing blockchain systems or complying with stringent AI transparency requirements can deter innovation and exclude smaller actors from the ecosystem. This reveals a critical gap in current regulatory approaches: the lack of tailored mechanisms to support social enterprises operating in resource-constrained environments.

²⁵ Vaño Vaño MJ (2015) 185-198. Casanovas Romeu (2012) 15-28. De Andrés Rivero, Hernández Marí (2009) 133-14.

Interoperability and technological neutrality are often celebrated as drivers of inclusivity, yet their potential remains underutilized. Standards and frameworks often prioritize technical efficiency over the realities faced by social entrepreneurs in underserved regions. For example, while initiatives such as e-CODEX and CEF Digital promote cross-border collaboration, they fail to address the systemic barriers that prevent equal participation, such as limited infrastructure and linguistic or cultural differences. These failures highlight the need for governance models that go beyond compliance and actively dismantle the structural inequalities embedded in the digital economy.

Equally troubling is the ethical dimension of these technologies. The adoption of AI and blockchain in social entrepreneurship poses risks of algorithmic discrimination, misuse of data, and loss of autonomy. Current regulations, such as the AI Act, focus heavily on mitigating high-risk applications, but fall short in addressing the systemic biases that pervade algorithmic decision-making processes. This regulatory oversight disproportionately affects vulnerable populations, who are often at the mercy of opaque systems with limited accountability.

Significant reforms are needed to ensure that the transformative potential of technology is aligned with the principles of social justice. These include the development of inclusive regulatory frameworks that prioritize the needs of marginalized communities, robust funding mechanisms to support the adoption of advanced technologies by smaller enterprises, and ethical safeguards that ensure transparency and fairness. Policymakers must adopt a proactive stance by anticipating and addressing the unintended consequences of technological innovations before they widen existing divides.

Ultimately, the success of interoperable technologies in social entrepreneurship depends on a paradigm shift: moving from a compliance-driven model to one rooted in equity, sustainability, and human rights. Collaboration between lawmakers, developers, and social actors is essential to building systems that not only comply with technical standards, but also uphold the dignity and agency of all users. Without this critical lens, the promise of digital transformation risks being reduced to a privilege for the few, rather than a tool for collective empowerment.

Bibliography

Ávila Gonzales, NP (2023) El comercio electrónico en Bolivia: el nuevo horizonte y sus desafíos jurídicos, Tesis Doctoral.

Belli L Foditsch N (2015) Network Neutrality. An Empirical Approach to Legal Interoperability. In: TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy Paper. <http://dx.doi.org/10.2139/ssrn.2588572>

Belli L, De Filippi P (2016) General Introduction: Towards a Multistakeholder Approach to Network Neutrality. In: Net Neutrality Compendium. Springer, Cham. https://doi.org/10.1007/978-3-319-26425-7_1

Casanovas Romeu P (2012) Some lines of research in legal knowledge management: semantic web, ODR and relational law. Scire: Representation and organization of knowledge. Zaragoza, 18(1): 15-28

De Andrés Rivero J, Hernández Marí R (2009) CRONOLEX: sistema para la representación dinámica de cuerpos legales. Scire: Representación y organización del conocimiento, Zaragoza, 15(1): 133-14

Gendler M (2015) What is Net Neutrality? Dangers and Potentialities,. <http://sedici.unlp.edu.ar/handle/10915/119990>

Gstrein, O. J., Haleem, N., & Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. *Internet Policy Review*, 13(3). <https://doi.org/10.14763/2024.3.1790>

Han, X., Gstrein, O. J., & Andrikopoulos, V. (2024). When we talk about Big Data, What do we really mean? Toward a more precise definition of Big Data. *Frontiers in Big Data*, 7, Article 1441869. <https://doi.org/10.3389/fdata.2024.1441869>

López Jiménez D (2019) Blockchain: technological, business and legal aspects, 79-119. <http://dx.doi.org/10.32870/Pk.a10n18.421>

Madrid Parra A (2003) Regulación internacional del comercio electrónico: Examen comparado de las leyes modelo de UNCITRAL. *Revista Aranzadi De Derecho y Nuevas Tecnologías*, 2: 15-41.

Madrid Parra A (2018) Contribución de la CNUDMI/UNCITRAL a la regulación del comercio electrónico. *Revista Aranzadi de Derecho y Nuevas Tecnologías*. 46

Madrid Parra A (2021) Fichas de dinero electrónico. Del dinero electrónico al "viejo" dinero digital. In: *Guía de Criptoactivos MiCA*, Aranzadi, Pamplona

Matter F (2016) A Regulatory Perspective on Net Neutrality. In: *Net Neutrality Compendium Human Rights, Free Competition and the Future of the Internet*, Springer, pp. 95-98. <https://link.springer.com/content/pdf/bfm:978-3-319-26425-7/2/1>

Meira, D., & Vañó Vañó, M. J. (2022). Empresas sociales en Portugal y España - un análisis comparativo. 33º *Congreso Internacional del CIRIEC. Valencia 13-15 junio de 2022* <http://ciriec.es/valencia2022/wp-content/uploads/COMUN-269.pdf>

Menéndez Mato JC, Gayo ME (2014): *Derecho e informática: Ética y legislación*. Bosch. Barcelona

Merchán Murillo A (2018) Digital Identity, Blockchain and e-Residency. <https://www.upo.es/investiga/derecho-nuevas-tecnologias/detallenoticias/Identidad-Digital-Blockchain-y-Residencia-Electronica/>

Merchán Murillo A (2019) Artificial intelligence and Blockchain: legal challenges in parallel. *RGDA*. 50

Monzón Campos, J. L., & Vañó Vañó, M. J. (2020). *Guía de Responsabilidad Social para las empresas y entidades de la Economía Social*. Valencia: CIRIEC-España, Centro Internacional de Investigación e Información sobre la Economía Pública, Social y Cooperativa.

Robles Carrillo M (2019) The net neutrality model in the European Union: scope and content. *European Community Law Review*. 63: 449-488. <https://doi.org/10.18042/cepc/rdce.63.03>.

Senent Vidal, M. J. & Ventura Franch A. (2024). Inteligencia artificial e igualdad de mujeres y hombres: una regulación jurídica necesaria. Especial referencia al proyecto de reglamento europeo. *IgualdadES*, 10, 45-71 doi: <https://doi.org/10.18042/cepc/IgdES.10.02>

Vañó Vañó, M. J., & Audivet M., Y.-D. (2023). Emprendimiento rural socialmente responsable a través de la colaboración público-privada mediante entidades de la economía social. Valencia:

CIRIEC-España, Centro Internacional de Investigación e Información sobre la Economía Pública, Social y Cooperativa. <https://ciriec.es/?descargar-publicacion=4046>

Vañó Vañó MJ (2005) XML, una herramienta al servicio del buen gobierno corporativo", Revista Aranzadi de derecho y nuevas tecnologías, 8:101-116

Vañó Vañó MJ (2008) La red europea LEXML: una integración de la documentación legal electrónica. In: El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos, p. 151-176

Vañó Vañó MJ (2009) Integration of electronic legal documentation through LEXML", Scire: Representation and organization of knowledge, 15(1):87-110

Vañó Vañó MJ (2012) Interoperability and publicity through the electronic business register. Scire. 18(1): 63-71. <https://ibersid.eu/ojs/index.php/scire/article/view/3996/3670>.

Vañó Vañó MJ (2015) Fraud prevention in electronic banking with legal and technological measures, In: Fraude Electrónico. Su gestión penal y Civil . Tirant lo Blanch, Valencia p. 201- 219

Vañó Vañó MJ (2015) XML application models in the legal field. In: Derecho y sistemas de datos: el uso del XML jurídico, Tirant lo Blanch, Valencia p. 185-198

Vañó Vañó MJ (2019) La vertebración de la economía social a través de las tecnologías de la información y de la comunicación". Noticias de la economía pública social y cooperativa = Noticias CIDEA, (62):42-48

Vañó Vañó MJ (2021) Blockchain, interoperabilidad y seguridad: oportunidad o fomento de la brecha digital. In: Retos del mercado financiero digital. Thomson Reuters Aranzadi. Cizur Menor.

Vargas Vasserot, C. (2022). Las empresas sociales como entidades de la economía social en el Plan de Acción Europeo. Propuestas lege ferenda para su reconocimiento en España en la Ley 5/2011 de Economía Social. CIRIEC-España, Revista Jurídica de Economía Social y Cooperativa (41), 289-329.

Wu T (2003) Network Neutrality, Broadband Discrimination. Journal of Telecommunications and High Technology Law, (2):141. <http://dx.doi.org/10.2139/ssrn.388863>

Zukerfeld M, Califano B (2019) Discussing net neutrality: from dominant discourses to practices in peripheral contexts. Commons. Journal of Communication and Digital Citizenship, 8(1), 5-43. <http://dx.doi.org/10.25267/COMMON.2019.v8.i1.01>