

Law into Code: EU Regulation of Digital Accountability Mechanisms for Responsible Business Conduct

By Tetiana Hudima¹, Anton Soshnykov², Viktor Dovhan³

ABSTRACT:

This article provides a legal analysis of digital mechanisms ensuring socially responsible business conduct in the context of economic digitalisation and the strengthening of regulatory requirements for sustainability, human rights, and environmental protection. It argues that contemporary digital technologies, such as algorithmic systems, digital ESG reporting, due diligence platforms, blockchain solutions, the Internet of Things, and platform accountability infrastructures, are no longer merely optional managerial tools. Instead, they increasingly acquire normative significance as integral components of compliance with legally binding obligations. The study applies a doctrinal, comparative, and functional methodology to examine digital mechanisms not only as technological solutions, but as functionally institutionalised forms of external control embedded in modern regulatory regimes. Particular attention is devoted to the regulatory framework of the European Union, including recent legal acts on corporate sustainability, due diligence, artificial intelligence, and digital services, which reflect a shift from ex post supervision towards preventive and continuous accountability implemented through digital infrastructures. The analysis demonstrates that digitalisation reshapes the functional structure of legal responsibility by transforming compliance into an ongoing, evidence-based, and technologically embedded process. The Ukrainian context is examined separately, with a focus on European integration and post-war recovery. The article identifies existing institutional preconditions for digital transparency in Ukraine, as well as systemic gaps hindering the formation of an integrated ecosystem of socially responsible business. It concludes that the integration of digital accountability mechanisms into legal regulation is a necessary condition for strengthening business responsibility, attracting sustainable investment, and aligning national regulatory frameworks with European Union standards.

Keywords: socially responsible management, sustainable development, legal regulation, business, supply chains, artificial intelligence, digital technologies (solutions), ESG, due diligence, blockchain.

1. Introduction

Digital technologies integrated into corporate activities increasingly acquire not only technical, but also normative significance in the field of corporate responsibility. Under contemporary conditions, the legal regulation of socially responsible business conduct is being supplemented by digital mechanisms designed to ensure transparency,

¹ Doctor of Legal Science, Professor, Deputy Head of the Department, «V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine», Kyiv, Ukraine, <https://orcid.org/0000-0003-1509-5180>

² PhD in Legal Sciences, Associate Professor, Senior Research Fellow, State Organization «V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine», Kyiv, Ukraine, <https://orcid.org/0000-0003-4998-9713>

³ PhD in Legal Sciences, doctoral student, State Organization «V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine», Kyiv, Ukraine, <https://orcid.org/0009-0004-4966-1253>

accountability, and due diligence. These mechanisms combine technological solutions, such as artificial intelligence, data analytics, blockchain, and the Internet of Things (IoT) with legally defined procedures of reporting, auditing, supervision, and liability.

As a result, technological instruments cease to be merely optional for business actors. Their use becomes part of the fulfilment of statutory obligations relating to human rights protection, environmental standards, business ethics, and transparency towards stakeholders. For instance, the Organisation for Economic Co-operation and Development (OECD) has noted that digital technologies, including blockchain, big data analytics, and artificial intelligence, are capable of strengthening integrity in supply chains by enhancing traceability, facilitating risk-related data exchange, and increasing supplier transparency, although they cannot fully substitute comprehensive due diligence processes (OECD. n.d.). Accordingly, digital solutions acquire a hybrid legal nature. On the one hand, they are grounded in purely technological processes, such as algorithms, digital platforms, and data registers. On the other hand, they are increasingly integrated into legal regimes of corporate governance, reporting, supervision, licensing, compliance, and the imposition of liability. This dual character underscores the need for comprehensive scholarly research into the digitalisation of socially responsible business conduct.

2. Literature Review

In scholarly literature, researchers examining socially responsible business conduct increasingly draw attention to the role of digital tools that contribute to the modernisation of approaches to implementing the contemporary concept of socially responsible economic activity (Abdallah-Ou-Moussa *et al.*, 2024; Jinyoung, 2024; Zheng *et al.*, 2023). Scholars analyse the impact of specific digital technologies on the development of socially responsible business practices and on enhancing the transparency and accountability of economic actors. In particular, E. Goodman and J. Trehu (2023), in their work “Algorithmic Auditing: Chasing AI Accountability”, examine the impact of artificial intelligence systems on the protection of human rights, emphasising the need for prior risk assessment of potential rights violations arising from their deployment. C. Swart and P. Zincone (2025) focus on the potential of artificial intelligence as a tool for the development and wider implementation of ESG reporting, particularly with regard to the automation of the collection, processing, and verification of non-financial data. Other scholars highlight the перспективність of blockchain technology in economic activity, notably for ensuring transparent and reliable monitoring of emissions volumes and compliance with environmental standards. At the same time, C. Pérez, I. López, and F. López (2025) examine the use of digital tools to ensure traceability of corporate actions, enhance supply-chain transparency, and strengthen trust among stakeholders. At the same time, it can be observed that the existing studies are largely fragmentary in nature and do not provide a holistic understanding of the role of digital tools in the formation and development of socially responsible economic activity, which substantiates the need for a comprehensive scholarly analysis of this issue.

3. Methodology

This study applies a complex socio-legal research methodology combining doctrinal legal analysis, comparative legal method, and functional analysis of digital technologies as regulatory instruments. The methodological framework is designed to capture the hybrid nature of digital mechanisms, which simultaneously operate as technological tools and legally relevant elements within contemporary systems of corporate social responsibility and sustainability regulation.

The core method of the research is doctrinal (dogmatic) legal analysis, used to examine the normative structure, legal objectives, and regulatory logic of European Union acts governing corporate sustainability, digital services, and artificial intelligence. This method enables the identification of binding legal obligations imposed on business entities and the legal status of digital mechanisms embedded within such obligations. Doctrinal analysis is applied to the examination of key EU legal instruments, including the Corporate Sustainability Reporting Directive (CSRD), the Corporate Sustainability Due Diligence Directive (CSDDD), the Artificial Intelligence Act (AI Act), and the Digital Services Act (DSA). The focus is placed on legal norms that either explicitly require the use of digital tools (such as machine-readable ESG reporting formats or algorithmic risk management systems) or implicitly rely on digital infrastructures for their practical enforcement. This allows the study to assess how digital technologies are transformed from optional managerial tools into legally significant compliance mechanisms.

The research employs a comparative legal method to analyse different regulatory models of socially responsible business and digital accountability across jurisdictions. The European Union regulatory framework is used as the primary reference model, while selected national regimes (notably Germany and France) are examined to illustrate how supranational standards are implemented through domestic legislation on supply-chain due diligence and corporate accountability. The comparative perspective is also extended to the Ukrainian legal context in order to assess the degree of normative convergence with EU standards and to identify structural gaps in the regulation of digital ESG reporting, due diligence obligations, and algorithmic accountability. This approach enables an evaluation of Ukraine's readiness to integrate into the European sustainability governance framework and highlights the legal and institutional adjustments required in the context of European integration and post-war reconstruction.

A functional legal analysis is used to examine digital technologies (such as algorithmic audits, blockchain, Internet of Things solutions, and digital ESG platforms) not as neutral technical tools but as functional components of legal regulation. This method focuses on the regulatory functions performed by digital mechanisms, including transparency enhancement, risk prevention, monitoring, evidence generation, and enforcement facilitation. By analysing the practical role of digital instruments in fulfilling legal obligations related to human rights protection, environmental compliance, and corporate governance, the study demonstrates how digitalisation reshapes traditional regulatory techniques. Particular attention is paid to the preventive and evidentiary functions of digital mechanisms, which increasingly replace ex post enforcement with continuous, technology-based compliance monitoring.

Given the inherently cross-sectoral nature of digital sustainability regulation, the research adopts an interdisciplinary approach, integrating insights from law and technology studies, sustainability governance, and digital compliance theory. This approach allows the study to assess not only the formal legal requirements but also the technological feasibility and regulatory consequences of embedding legal norms into digital systems. The analysis is conducted within a broader contextual framework, taking into account current economic, technological, and geopolitical conditions, including the digital transformation of markets, the extraterritorial impact of EU law, and the specific challenges of corporate accountability in post-conflict reconstruction environments. This contextualisation ensures that the findings reflect real regulatory dynamics rather than abstract normative models.

The study is primarily based on normative and qualitative legal analysis and does not include empirical data collection or quantitative assessment of corporate practices. While this approach allows for an in-depth examination of regulatory models and legal concepts, it does not measure the effectiveness of digital mechanisms in practice. Nevertheless, the chosen methodology is appropriate for the article's objective, which is to conceptualise digital mechanisms as elements of legal regulation and to identify structural trends in the evolution of socially responsible business governance.

4. Result

4.1. Digital mechanisms of socially responsible business conduct: legal framework

Within the European legal framework, digital mechanisms of socially responsible business conduct are closely linked to the implementation of international due diligence standards (most notably the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD, 2023), as well as to recent EU regulatory instruments with extraterritorial reach. In particular, Directive (EU) 2022/2464 on corporate sustainability reporting obliges thousands of companies, including non-EU undertakings, to disclose standardised ESG information. At the same time, Directive (EU) 2024/1760 on corporate sustainability due diligence requires large companies, including those established in third countries, to carry out continuous monitoring of their impacts on human rights and the environment across their entire chains of activities (Debevoise & Plimpton LLP, 2023). This regulatory shift transforms corporate legal responsibility from compliance based on periodic ex post checks into a model of continuous, technology-mediated oversight. In practical terms, this affects companies' everyday legal duties by requiring ongoing risk monitoring, systematic documentation of due diligence processes, and the generation of digital evidence relevant for compliance assessment and potential liability.

In addition, national legislation, such as the German Act on Corporate Due Diligence Obligations in Supply Chains (*Lieferkettensorgfaltspflichtengesetz*, LkSG, 2021 (Government of Germany, 2021) and the French Duty of Vigilance Law applicable to parent companies and ordering undertakings (*Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre* (Government of France, 2017)) establishes binding legal requirements for the monitoring of suppliers and relies on digital instruments for their practical implementation, including counterparty screening platforms and compliance tracking systems. Within the field of IT and platform regulation, digital

accountability mechanisms are reflected in legal norms governing algorithmic systems (covering, *inter alia*, the regulation of artificial intelligence, personal data protection, and requirements of algorithmic transparency and explainability) as well as in rules on platform accountability under the EU Digital Services Act (European Parliament & Council of the European Union, 2022a)). The following section examines the key categories of digital mechanisms supporting socially responsible business conduct. For clarity, the main categories of digital accountability mechanisms and their core legal functions are summarised in Table 1, including algorithmic audits, digital ESG reporting, blockchain- and IoT-based traceability tools, online platform accountability frameworks, and digital due diligence instruments, with separate attention devoted to the Ukrainian context of their application.

Table 1. Digital accountability mechanisms and their legal functions

Digital mechanism	Core legal function	Key EU instruments
Algorithmic audits	Preventive oversight, compliance control	AI Act, DSA
Digital ESG reporting	Transparency and disclosure	CSRD
Digital due diligence tools	Risk monitoring and evidence generation	CSDDDD
Blockchain & IoT	Traceability and proof	CSDDDD, sectoral regulation
Platform accountability	Systemic risk governance	DSA

Digital mechanisms for ensuring socially responsible business conduct may be understood as normatively regulated (or normatively relevant) modes of using digital technologies aimed at fulfilling corporate obligations relating to risk management, respect for human rights, environmental standards, corporate ethics, and transparency in relations with stakeholders. In this sense, they constitute technical instruments that are directly or indirectly embedded in the implementation of legal norms governing corporate social responsibility. Such mechanisms possess a dual nature. They are, at the same time, the outcome of technological innovation (algorithms, digital platforms, and data registers) and integral components of the legal regulatory framework, insofar as legislation and regulatory policies increasingly require or incentivise their use in order to achieve normative objectives. In particular, the European Commission has explicitly emphasised in its digital strategies that contemporary regulation should ensure the technical integration of accountability principles, for example through mandatory algorithmic audits, disclosure requirements concerning the operation of digital platforms, and the use of standardised data formats for ESG reporting (European Commission, n.d.). Accordingly, digital solutions are increasingly becoming institutionalised within the legal framework. What initially emerged as private or voluntary initiatives is gradually evolving into mandatory mechanisms explicitly provided for by legislation.

The place of digital mechanisms within the system of legal regulation of socially responsible business conduct is determined by their functional role. They form part of a broader legal framework aimed at ensuring the fulfilment of corporate obligations in the fields of environmental protection, human rights, and business integrity. For example, the

due diligence requirement in supply chains, as enshrined in the CSDDD, can in practice be implemented only through digital instruments for collecting and analysing supplier-related data, such as IT platforms, data registers, and automated screening systems (OECD, n.d.). Similarly, the expanding obligations of non-financial (ESG) reporting under the CSRD are directly linked to the introduction of a digital reporting format (XBRL) and the establishment of EU-wide access to such data. In this way, digital mechanisms perform the function of a connecting link between the technological practices of undertakings and the normative objectives of the state and society in the fields of sustainable development and human rights. Their emergence signifies a transition to a new regulatory model in which control and accountability are to a significant extent exercised through procedures embedded in IT systems, rather than through purely documentary or ex post forms of verification that characterised earlier regulatory approaches.

4.2. Algorithmic auditing as a legal mechanism of accountability

One of the key digital mechanisms is algorithmic auditing, understood as independent assessments of automated systems (primarily artificial intelligence systems) for compliance with specific ethical and legal criteria, such as non-discrimination, transparency, reliability, and safety. The significance of algorithmic audits has increased substantially following the adoption of the Artificial Intelligence Act and the Digital Services Act, both of which introduce mandatory procedures for the assessment and auditing of algorithmic systems (European Parliament & Council of the European Union, 2022) and the DSA, both of which introduce mandatory procedures for the assessment and auditing of algorithmic systems.

The AI Act establishes a risk-based approach to artificial intelligence, under which AI systems classified as high-risk are subject to stringent requirements prior to being placed on the market. These requirements include the establishment of risk management systems, the assurance of data quality, the preparation of technical documentation, the logging of system operations, transparency towards users, and mandatory human oversight of outcomes (Articles 9–15 of the AI Act). Compliance with these requirements is ensured through conformity assessment procedures, which involve either internal or external audits of algorithmic systems aimed at verifying adherence to the prescribed criteria before deployment and on a periodic basis thereafter (Council of the European Union, 2024, May 21). In practical terms, companies prepare for such audits by implementing internal governance structures, maintaining audit-ready technical documentation, and integrating compliance-by-design mechanisms throughout the AI system lifecycle (Veale & Borgesius, 2021). Regulatory consistency across sectors is ensured through harmonised risk classification, standardised conformity assessment procedures, and the oversight of designated supervisory authorities under the AI Act. In legal doctrine, such assessments are regarded as a form of algorithmic auditing, insofar as they involve a structured and independent evaluation of artificial intelligence systems in their actual context of use, aimed at identifying and documenting risks to human rights and interests, including discrimination, bias, and infringements of privacy. Scholars emphasise that algorithmic auditing encompasses multiple dimensions of AI operation, ranging from the examination of training data and models (particularly for the detection of bias) to the assessment of the system's broader impacts on users and society (Goodman & Trehu, 2023). Scholars

emphasise that algorithmic auditing encompasses multiple dimensions of AI operation, ranging from the examination of training data and models (particularly for the detection of bias) to the assessment of the system's broader impacts on users and society (Caplan et al., 2018)). Accordingly, the AI Act effectively institutionalises algorithmic auditing as a mechanism of preventive oversight over high-risk technologies.

The DSA introduces, for the first time at the normative level, a system of mandatory annual independent audits for very large online platforms and very large online search engines (the so-called VLOPs and VLOSEs (European Commission, n.d.), with an audience exceeding 45 million users in the EU). Pursuant to Article 37 of the DSA, such entities are required to engage independent qualified auditors at least once a year in order to assess their compliance with the Regulation, including the effectiveness of risk management systems, content moderation procedures, and advertising algorithms. The results of the audit are formalised in an audit report containing recommendations, and the platform is required to adopt corrective measures on the basis of the audit findings (European Commission, n.d.). The primary objective of these audits is to enhance the transparency and accountability of major digital market actors, in particular by enabling independent verification of their claims regarding the management of systemic risks on their platforms.

The scope of issues covered by DSA audits is directly linked to corporate social responsibility in the online environment. Auditors examine, inter alia, whether platforms take adequate measures to combat illegal content, disinformation, and hate speech; whether they ensure transparency of recommendation systems and targeted advertising; and how they protect users' rights, including those of vulnerable groups and minors (MediaLaws, n.d.). Accordingly, auditors assess not only the technical functioning of platforms but also the ethical and social risks associated with their operation, thereby compelling platforms to raise their standards of responsibility.

From a legal perspective, algorithmic auditing performs several important functions. First, it fulfils a control function, ensuring independent external oversight of a company's compliance with its legal obligations through the involvement of third-party auditors. Second, it serves a preventive function, as regular assessments make it possible to identify risks at an early stage and to prevent future violations or reputational scandals. Third, algorithmic auditing performs an evidentiary function, since audit findings are documented in reports that may serve as a basis of proof in disputes concerning corporate responsibility, including proceedings before regulatory authorities or courts. Fourth, it fulfils a communicative function, insofar as audit conclusions (often published at least in the form of non-exhaustive summaries (shape the informational environment for investors, consumers, and the public regarding a company's integrity. Accordingly, algorithmic audits today constitute not merely an instrument of internal control, but a legal institution aimed at ensuring the accountability of digital services to society.

For Ukraine, the introduction of algorithmic auditing into national practice represents a particularly relevant issue. Although Ukrainian legislation currently does not impose a direct obligation to audit algorithmic systems, developments at the EU level increasingly prompt consideration of the future implementation of comparable mechanisms. Sectors in which such requirements may become necessary in the near term include banking and financial services (such as credit scoring models and fraud-monitoring

systems), insurance, electronic commerce, and online platforms. Implementation may take place either through the adoption of explicit legal provisions (for example, within legislation on payment systems or data protection in the course of aligning national law with EU rules on artificial intelligence) or through the voluntary uptake of auditing practices by companies seeking to enhance trust among customers and business partners.

4.3. Digital ESG reporting as an instrument of transparency and disclosure

Another key mechanism is digital ESG reporting, that is, reporting on environmental, social, and governance aspects of corporate activity. Within the European Union, this form of reporting is undergoing a transition from a largely voluntary practice to a mandatory and standardised regime applicable to a broad range of undertakings. The central legal instrument in this area is Directive (EU) 2022/2464 on corporate sustainability reporting (European Parliament & Council of the European Union, 2022), which has significantly expanded the scope of reporting entities compared to the former Non-Financial Reporting Directive 2014/95/EU. Under the CSRD, large companies as well as all publicly listed companies (with the exception of small undertakings) are required to disclose detailed sustainability-related information in accordance with the European Sustainability Reporting Standards (ESRS). Such reports must cover, *inter alia*, the environmental and climate impacts of corporate activities, respect for human and labour rights, gender equality and broader social issues, anti-corruption measures, and corporate governance structures (BDO in Ukraine, n.d.). Importantly, the CSRD is explicitly oriented towards a digital reporting model. Sustainability reports are to be submitted in a machine-readable format (expected to rely on the XBRL standard) and made publicly accessible through the European Single Access Point. As a result, ESG data effectively become part of a large-scale digital information infrastructure that can be automatically processed by regulators, analysts, and the public.

The digitalisation of non-financial reporting serves several interconnected objectives. First, it enhances regulatory oversight. Financial, environmental, and other supervisory authorities gain rapid access to standardised corporate data, enabling them to more easily identify inconsistencies with declared sustainability targets or instances of non-compliance, such as excessive emissions or the existence of litigation related to labour rights. Second, digitalisation promotes comparability and analytical capacity. Harmonised digital data make it possible to compare sustainability indicators across companies and sectors, construct rankings and indices, and identify market-wide correlations. Third, digital ESG reporting facilitates integration into financial decision-making. As scholars rightly observe, only digitised ESG indicators can function as a genuine regulatory resource capable of being incorporated into financial regulation, credit ratings, investor decision-making, and public support schemes (Swart & Zincume, 2025). When sustainability-related information is available in near real-time to banks, investment funds, or public authorities, it can be more effectively taken into account in lending decisions, portfolio construction, or the granting of public guarantees. For this reason, the European Union places particular emphasis on the digital format of ESG reporting. As a result, ESG data become an integral component of the broader digital ecosystem of financial information.

For Ukraine, the implementation of digital ESG reporting is of dual relevance. On the one hand, it is driven by the direct impact of EU law. In particular, Ukrainian

companies whose securities are traded on European markets, or which form part of corporate groups with parent companies established in the EU, will be required to report in accordance with the CSRD and the ESRS between 2025 and 2028, depending on their respective category (BDO in Ukraine, n.d.). On the other hand, even companies operating exclusively on the domestic market will be affected indirectly, as Ukraine's European integration entails the gradual harmonisation of reporting requirements. In this regard, in October 2024 the Government of Ukraine approved a Strategy for the introduction of sustainability reporting (Cabinet of Ministers of Ukraine, 2024) by undertakings in line with the CSRD and the ESRS (BDO in Ukraine, n.d.). A phased introduction of mandatory non-financial reporting in Ukraine is therefore expected, including the use of digital formats for the submission and publication of data. Accordingly, businesses should already begin preparing for the forthcoming requirements, *inter alia* by reviewing their internal IT systems for data collection, training personnel in ESG reporting, and implementing software solutions for the automated calculation of sustainability indicators. Such preparation has not only a regulatory, but also a strategic dimension. Companies that successfully digitise and transparently disclose their ESG performance are likely to gain improved access to European capital markets and partnership opportunities (BDO in Ukraine, n.d.).

It should be noted that the implementation of the CSRD within the European Union has been accompanied by discussions concerning the possible simplification or postponement of certain requirements, particularly for small and medium-sized enterprises. In 2025, the European Commission signalled its readiness to introduce phase-in periods and to simplify selected indicators for smaller undertakings in response to concerns about excessive regulatory burdens (BDO in Ukraine, n.d.). Nevertheless, the strategic commitment to comprehensive transparency and the digitalisation of non-financial information remains unchanged. Even where implementation timelines are adjusted, the global trend clearly points towards enhanced corporate transparency and the digital disclosure of social and environmental performance indicators. For Ukrainian public policy, this implies the need to develop, as a matter of priority, the institutional and technical infrastructure required for the collection and analysis of such data. This includes the establishment of public registers for ESG reports, integration with existing financial reporting registers, and capacity-building for regulatory authorities to work effectively with digital reporting formats such as XBRL.

4.4 Blockchain- and IoT-based traceability tools

Digital mechanisms of socially responsible business conduct also include blockchain technologies and the IoT, which enable reliable data recording and the traceability of events within economic activities. Their use is particularly promising for verifying compliance with corporate obligations in the fields of human rights, ethical supply-chain practices, and environmental protection.

Blockchain is a distributed ledger technology that enables data to be recorded in an immutable manner with a high degree of trust. In the context of socially responsible business conduct, blockchain is primarily used for supply-chain traceability and the verification of product origin. According to assessments by the World Economic Forum, digital platforms (particularly those based on distributed ledger technologies) are

contributing to the emergence of a new model of trust in supply chains by providing a “single version of the truth” and ensuring shared access to data on participants and transactions for all relevant stakeholders. This, in turn, creates technological preconditions for enhanced transparency with regard to environmental and labour-related risks (World Economic Forum, 2020). In addition, blockchain may be used for the registration of carbon credits and the monitoring of greenhouse gas emissions (Merlo *et al.*, 2025). Companies record their emission levels and emission-reduction projects in secure distributed registers, which enables auditors and regulators to verify the accuracy and reliability of the reported data. In the contractual sphere, smart contracts (algorithmic protocols based on blockchain technology) are capable of automatically enforcing environmental or social clauses of agreements. For example, such mechanisms may trigger the allocation of funds to environmental initiatives when predefined emission thresholds are exceeded.

In turn, the IoT, that is, a network of sensors and devices capable of collecting data in real time, serves as a functional complement to blockchain by providing a digital interface with the physical world. Through IoT sensors deployed in production facilities or during transportation, it becomes possible to monitor working conditions, energy consumption, emission levels or pollutant discharges, as well as logistical parameters such as transport routes and conditions. The data collected may be automatically transmitted to secure databases or blockchain-based registers, thereby enabling the continuous recording and verification of compliance with applicable standards, including temperature, environmental, and safety requirements. This approach has already been examined in academic literature, which highlights the combined use of IoT and blockchain technologies for environmental monitoring, supply-chain traceability, and the enhancement of corporate environmental responsibility (Ajakwe *et al.*, 2025; Soori *et al.*, 2024).

The legal significance of data collected through blockchain and IoT technologies depends on their authenticity and admissibility in legal proceedings. Where a technological solution ensures a sufficient level of data trustworthiness, namely, protection against tampering, alteration, or loss, such records may be recognised as evidence of a company’s compliance with, or breach of, its legal obligations. European legislation is gradually moving towards the recognition of blockchain-based records in specific regulatory contexts. An example is the pilot regime for market infrastructures based on distributed ledger technology established by Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022. At the same time, the use of blockchain and IoT raises a number of new legal challenges, including the protection of personal data (given that unrestricted public access to distributed registers may conflict with the General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union., 2016), as well as cybersecurity concerns, such as vulnerabilities in IoT devices or smart contracts, and questions of liability for technical failures, including situations where automated mechanisms malfunction or produce erroneous outcomes. Legal scholars note that blockchain records, by virtue of their characteristics of immutability and timestamping, may function as techno-legal evidence capable of facilitating the demonstration of due diligence in supply chains. Nevertheless, their ultimate evidentiary value will depend on judicial assessment, compliance with procedural rules of evidence,

and the specific factual context in which such records are relied upon (European Law Institute, 2022).

Accordingly, blockchain and IoT technologies perform the function of a digital infrastructure of trust in the sphere of responsible business conduct. They provide a level of transparency and controllability that was previously unattainable in global supply chains. For businesses, these technologies increasingly operate as a form of a “digital shield” against risk. In particular, by investing in traceability systems, a company not only reduces the likelihood of actual violations, but also strengthens its protection against reputational and legal losses in the event of incidents, as it is able to demonstrate objective and verifiable data concerning its conduct.

4.5 Platform accountability under the Digital Services Act

The development of the platform economy, marked by the growing dominance of online platforms in areas such as commerce, media, and labour, brings the issue of their social responsibility to the forefront. Large digital platforms exert an influence on society comparable to that of public institutions, which necessitates legal regulation aimed at ensuring their accountability to public interests. In this context, the European Union adopted the DSA in 2022, introducing a comprehensive set of obligations for platforms and intermediary services. Specific and heightened obligations are imposed on very large online platforms (VLOPs) and very large online search engines (VLOSEs), as noted above, in view of the significant societal impact associated with the scale of their audiences.

The key mechanisms of platform accountability under the DSA include:

(1) systemic risk assessment – very large online platforms and very large online search engines (VLOPs/VLOSEs) are required to carry out an annual self-assessment of systemic risks associated with the functioning of their services. Such risks include, *inter alia*, the dissemination of illegal or harmful content, threats to fundamental rights (such as freedom of expression and non-discrimination), manipulation of electoral processes, and risks to mental health (European Commission. n.d.). The resulting risk assessment report must be submitted to the European Commission and the competent supervisory authorities.

(2) risk mitigation measures – on the basis of the risk assessment, platforms are required to adopt proportionate mitigation measures in order to reduce the identified risks (Article 35 of the DSA). Such measures may include modifications to recommendation algorithms where they contribute to the dissemination of polarising content, enhanced content moderation practices, restrictions on targeted advertising in relation to vulnerable groups, and the redesign of user interfaces aimed at reducing addictive or harmful user behaviours (European Commission. n.d.).

(3) independent auditing – as noted above, the DSA (Article 37) requires VLOPs and VLOSEs to undergo an annual external audit assessing compliance with obligations relating to transparency, risk management, and the protection of fundamental rights. The audit report identifies deficiencies and provides recommendations for improvement. Failure to implement such recommendations exposes platforms to the risk of sanctions, thereby rendering auditing an enforcement-oriented mechanism of regulatory change.

(4) algorithmic and advertising transparency – the DSA (Article 39) introduces unprecedented obligations concerning the disclosure of information about algorithmic

systems. Platforms are required to explain to users the main parameters and principles underlying the functioning of their recommender systems, for example the signals on which news feeds or video recommendations are based. In addition, the Regulation establishes public repositories of online advertising, in which VLOPs must store information on all advertisements displayed on their services, including their duration, targeting audience, and content (European Commission. n.d.). These requirements significantly enhance transparency in the online advertising ecosystem and make manipulative practices more difficult to sustain.

5) access to data and verification. In order to strengthen external accountability, the DSA grants accredited researchers access to certain internal platform data for the purpose of scientific analysis of systemic risks and societal impacts (Article 40 of the DSA) European Commission. n.d.). This mechanism addresses the longstanding problem whereby platforms previously held exclusive control over information concerning their algorithmic systems and were able to interpret their operation without independent verification.

Compliance with these requirements is already producing tangible legal consequences. Between 2023 and 2025, the European Commission initiated the first investigations into potential non-compliance with the DSA by several major technology companies, notably in relation to content moderation practices and online advertising on widely used social media platforms. Sanctions under the DSA may reach up to 6% of a company's global annual turnover (Article 74), which confers substantial normative weight on these obligations. Accordingly, platform accountability is evolving from a political aspiration into a concrete legal regime that integrates elements of corporate responsibility into the regulation of digital services. In effect, the European Union is establishing a new standard of socially responsible business conduct for online intermediaries, emphasising that the freedom of internet-based business activities must be accompanied by responsibility towards society for their potential negative externalities.

For Ukrainian companies that interact with European platforms (for example, by selling goods on online marketplaces or providing content to social media services) this entails the need to take the rules of the DSA into account in their business activities. Where platforms adjust their algorithms or revise requirements for business users in order to comply with the DSA, Ukrainian partners must be prepared to adapt accordingly. Moreover, in the context of Ukraine's prospective accession to the European Union, the provisions of the DSA and related regulatory acts are likely to become binding within the national legal order. Against this background, it is already advisable for Ukrainian businesses to study practices of platform accountability and to engage in initiatives of online business self-regulation, such as codes of conduct addressing disinformation. Such proactive adaptation would facilitate the development of Ukraine's digital business sector in line with European standards of responsibility and accountability.

4.6. Digital due diligence and evidence generation

Human rights and environmental due diligence have become one of the central requirements of responsible business conduct in the 2020s. A clear shift is taking place from traditional declarations of corporate social responsibility towards legally binding regimes governing the monitoring of suppliers and business partners. This transition is to

a significant extent enabled by digital mechanisms, as the manual identification and monitoring of potential violations at every stage of global supply chains is practically unfeasible.

As noted above, in 2024 the European Union adopted the CSDDD (White & Case, 2024). The Directive obliges large companies (at the first stage (from 2027) those with a net turnover exceeding EUR 1.5 billion and more than 5,000 employees, and from 2029 those with a turnover exceeding EUR 450 million and more than 1,000 employees) to integrate into their business operations policies and procedures aimed at identifying, preventing, mitigating, and remedying adverse impacts on human rights and the environment, as well as to report on the measures taken. The due diligence obligation extends to the company's entire "chain of activities", encompassing its own operations, subsidiaries, and supply chains, including suppliers, subcontractors, and, to a certain extent, distributors (White & Case, 2024). A comparable regulatory approach is already reflected in German law. The German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz, LkSG), in force since 2023, applies to companies employing more than 3,000 workers and requires the establishment of risk management systems in supply chains, the designation of a responsible officer, the conduct of annual risk analyses concerning human rights and environmental violations, the introduction of grievance mechanisms, and the publication of reports on due diligence measures (Taylor Wessing, 2021).

In practice, these regulatory requirements are virtually impossible to fulfil without the use of advanced IT solutions. The experience of large companies in the European Union and the United States demonstrates that effective supply chain due diligence relies on the deployment of the following digital tools and systems:

1) specialised supplier monitoring platforms. The market has seen the emergence of dedicated software-as-a-service (SaaS) (Net Help, 2025, August 17)), solutions that aggregate data on suppliers from multiple sources, including public registers, media reports, and sanctions databases, and assign risk scores accordingly. Well-known providers such as EcoVadis (EcoVadis. n.d.), IntegrityNext (ISPnext, n.d.) offer digital platforms that enable companies to monitor the sustainability profiles of their business partners in real time. These systems automatically generate alerts when adverse information emerges in relation to a supplier, for example, labour disputes or environmental incidents, or when required documentation has not been updated.

2) automated counterparty screening tools. For baseline supplier screening, companies rely on online registers and databases, including sanctions lists, court registries, debtor registers, and certification databases (such as International Organization for Standardization and Fairtrade). In many jurisdictions, such data are accessible via APIs, enabling large companies to configure automated data collection for each new counterparty, including checks on sanctions exposure, the existence of environmental permits, and the identification of ultimate beneficial owners. In Ukraine, for example, open data from the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Associations contain information on beneficial ownership, allowing businesses to assess suppliers' ownership structures and identify potential links to persons associated with reputational or compliance risks (OpenOwnership, n.d.).

3) digital trackers and product passports. A particularly recent development is the introduction of digital product passports, often based on blockchain technology, which record information on the origin, materials, and certification of each individual product. In certain sectors (most notably electronics and batteries) the European Union plans to make such product passports mandatory (European Parliament & Council of the European Union, 2023). This will require suppliers to integrate into a digital value chain by providing standardised product data in a unified format. When combined with IoT technologies, such as sensors embedded in goods or transport units, digital product passports enable end-to-end traceability from raw materials to the final consumer. This allows for the continuous recording of potential risks, including the use of illegally sourced materials or breaches of temperature and safety conditions during transportation.

Overall, the digitalisation of due diligence procedures renders them scalable and continuous. Whereas supplier audits were previously conducted selectively and at multi-year intervals, leading companies now seek to monitor the current risk profile of their supply chains on an ongoing basis through digital dashboards. This development also alters the legal nature of the due diligence obligation itself. Due diligence is transformed from a one-off verification exercise into a continuous process supported by IT systems. In the context of judicial proceedings or enforcement actions, decisive importance is attached not merely to the formal existence of corporate policies, but to the ability to demonstrate the actual implementation of due diligence requirements through monitoring and data-recording systems. The deployment of digital control mechanisms can therefore strengthen a company's evidentiary position, as recorded data provide traceability and immutability of information (Pérez *et al.*, 2025). By contrast, reliance solely on paper-based policies does not constitute sufficient proof of having exercised appropriate due diligence.

For Ukraine, although the CSDDD will not apply directly until EU accession, its impact is already tangible. Ukrainian exporters increasingly face requests from European partners to disclose environmental and social practices, provide supply chain data, and participate in digital supplier monitoring systems. This reflects a market-driven compliance effect, whereby access to European value chains depends on meeting due diligence standards implemented through digital platforms. Accordingly, Ukrainian businesses must prepare for a "digital filter" in export activities by investing in process transparency, systematic tracking of labour and environmental indicators, and the digitalisation of documentation. Given the likelihood that these requirements will intensify, public authorities may support this transition through targeted training programmes and the development of national digital infrastructures, such as registries of exporters that have demonstrated compliance with social responsibility and due diligence standards.

In Ukraine, the implementation of digital mechanisms of social responsibility remains fragmented, although certain elements are already in place. At the same time, digital mechanisms of socially responsible business conduct acquire particular significance in the context of financing Ukraine's recovery projects, both in the current phase and in the post-war period. Substantial volumes of international financial assistance, loans, and investments directed towards the reconstruction of infrastructure, housing, energy, and industry are accompanied by heightened requirements for transparency, accountability, and integrity in the use of funds. International donors and international financial institutions increasingly link access to financing to compliance with ESG principles, the

existence of due diligence systems, digital reporting, and effective mechanisms for monitoring project implementation. In this context, digital platforms, public registers, and data analytics tools become a precondition for access to recovery funding, as they enable traceability of financial flows, reduce corruption risks, and enhance investor confidence. Accordingly, the digitalisation of socially responsible business conduct in Ukraine constitutes a key factor not only for legal and institutional convergence with the European Union, but also for the effective mobilisation and use of resources necessary for the country's sustainable recovery.

In this respect, several specific digital instruments of social responsibility can be identified in Ukraine. These include electronic financial reporting systems, through which businesses submit financial and tax reports online, *inter alia* via the Electronic Taxpayer's Cabinet and the financial reporting systems administered by the National Bank of Ukraine. Although these instruments primarily serve the purpose of financial transparency, they simultaneously establish the digital infrastructure necessary for the collection and integration of non-financial and ESG-related data. Another important element is public open registers. Ukraine was among the first countries worldwide to provide open access to its business register and information on ultimate beneficial owners as early as 2015, which constitutes a significant anti-corruption measure and creates essential preconditions for transparency and accountability in business activities (Markle, n.d.).

In addition, Ukraine operates the Unified State Register of Court Decisions, which enables the verification of a counterparty's litigation history, the Unified Register of Environmental Impact Assessment containing reports on the environmental effects of business activities, as well as a number of other public databases. These instruments enhance the transparency of the business environment and facilitate data collection for due diligence purposes. The electronic public procurement system ProZorro, frequently cited as a benchmark for digital transparency, has since 2016 ensured that all public procurement procedures are conducted online with full access to documentation, participants, and outcomes. The transparency principle has significantly reduced corruption risks and generated substantial savings. This experience demonstrates that a digital platform operating under mandatory rules, as established by the Law of Ukraine "On Public Procurement", can markedly enhance integrity across a broad range of state-related economic transactions. While ProZorro is currently adapting to wartime conditions, it continues to preserve its core principles of openness and transparency (Legal 500, n.d.). Non-financial reporting initiatives are also emerging in Ukraine. Although no law on mandatory ESG reporting has yet been adopted, some Ukrainian companies voluntarily publish non-financial reports, most notably in the public sector and among subsidiaries of multinational corporations. At the state level, as noted above, in October 2024 the Cabinet of Ministers of Ukraine adopted the Strategy for the Introduction of Corporate Sustainability Reporting (Cabinet of Ministers of Ukraine, 2024). In other words, a regulatory and legal framework is currently being prepared to enable the introduction of mandatory sustainability reporting in the future.

At the same time, a comprehensive regime of digital mechanisms for socially responsible business conduct has not yet been established in Ukraine. One of the key challenges in this respect concerns non-financial reporting. The absence of a specific law or mandatory standard renders such reporting purely voluntary. As a result, companies do

not follow a unified disclosure format, while the use of digital instruments, such as XBRL International or other digital taxonomies for sustainability indicators, remains rather limited. In this context, the introduction of mandatory ESG disclosure requirements, at least at the level of the capital markets, appears particularly relevant.

Second, due diligence. For Ukrainian law, this concept remains relatively new. Existing legislation in the fields of labour, environmental protection, and human rights establishes general standards of conduct for businesses, but does not impose direct liability on companies for violations committed by their contractors or suppliers within supply chains. In the context of approximation to EU law, the introduction of rules requiring large companies to conduct supply chain due diligence will become unavoidable. The implementation of such obligations will also necessitate the development of appropriate digital tools, including domestic IT solutions or the adaptation of foreign platforms to Ukrainian conditions, for example through voluntary national portals of certified suppliers.

Third, algorithmic ethics. Current Ukrainian legislation in the field of digital technologies, including laws “On electronic communications” (Verkhovna Rada of Ukraine, (2020)), and “On personal data protection” (Verkhovna Rada of Ukraine, 2010) does not contain specific requirements concerning algorithmic transparency, the use of artificial intelligence systems, or the ethical dimensions of automated decision-making. At the same time, comprehensive regulation in this area is already emerging at the international level, particularly within the European Union, and its elements will require future implementation in national law. In this context, the proactive adoption of professional standards and guidelines for the ethical use of algorithms by Ukrainian companies (for example, AI ethics codes in the banking sector or human resources management) appears advisable, as it would facilitate preparation for forthcoming legislative changes and enhance the investment attractiveness of the Ukrainian market.

In summary, the Ukrainian context is currently characterised by the presence of individual components (such as electronic registers, ProZorro, and electronic reporting systems) while lacking their integration into a coherent ecosystem of socially responsible business. European integration will undoubtedly act as a catalyst for the formation of such an ecosystem. It is therefore advisable to institutionalise this agenda at an early stage, including the designation of a central executive authority responsible for the implementation of ESG standards and the coordination of due diligence approaches (for example, the Ministry of Economy, Environment and Agriculture of Ukraine). Particular attention should also be paid to the development of technical infrastructure, such as the establishment of a national sustainability information portal through which companies would submit non-financial data and the public would have user-friendly access to such information. This would enhance trust in business and facilitate alignment with EU standards.

The analysis demonstrates that digital mechanisms perform a range of functions within the system of legal regulation of corporate sustainability and business social responsibility.

First, they fulfil an information transparency function (or information openness function), by ensuring broad access to data on corporate activities. Digital ESG reporting and open public registers reduce information asymmetries between companies and stakeholders (Debevoise & Plimpton LLP, 2023). Whereas public oversight previously

relied largely on voluntary disclosures or investigations conducted by civil society organisations and journalists, digital mechanisms now provide systematised and standardised information. This enhances market discipline, as companies engaged in unethical practices or causing adverse environmental impacts can no longer remain opaque, while investors and consumers gain effective tools to identify such actors and apply economic pressure, including by limiting or terminating business relations.

Second, the supervisory (control) function. Digital mechanisms significantly enhance the capacity of regulators and auditors to oversee business conduct. Algorithmic audits under the AI Act and the DSA, due diligence assessments under the CSDDD, and sustainability reporting audits under the CSRD function as instruments of external control that were previously weak or largely absent (MediaLaws, n.d.). Regulators are no longer limited to reliance on corporate self-reporting, but may initiate independent audits and obtain access to internal data, thereby increasing the likelihood of detecting violations and strengthening enforcement credibility.

Third, the preventive function. Digital tools enable the prevention of many violations rather than their mere *ex post* identification. Real-time risk monitoring systems (such as supplier platforms or IoT-based emissions monitoring) allow potential issues to be detected before material harm occurs (Martín-Baos et al., 2022; Meena et al., 2022; Ramadan et al., 2024). This enables companies to identify “weak links” and take corrective action, for example by replacing unreliable suppliers or adjusting algorithms, prior to the emergence of legal liability or reputational damage. Such a proactive approach constitutes a core element of contemporary corporate responsibility culture.

Fourth, the evidentiary function. Digital traces and records create a body of objective evidence that may be relied upon in dispute resolution and enforcement proceedings. For example, blockchain records of raw material supplies may demonstrate that a company did not use illegally sourced inputs, while logs of automated systems may show what measures were taken to prevent discriminatory practices. The availability of such evidence strengthens the rule of law by reducing reliance on assumptions and increasing dependence on technologically recorded facts. At the same time, it raises legal requirements for digital systems themselves, as their reliability and protection against manipulation acquire direct legal significance.

Fifth, the integrative function. Digital mechanisms connect different branches of law by operating at their intersection. For instance, ESG reporting platforms simultaneously engage corporate law (disclosure obligations), environmental law (environmental data), and labour law (workforce-related indicators). Similarly, algorithmic requirements under the AI Act combine elements of IT law, human rights protection, and market regulation. Through digital infrastructures, regulation increasingly takes the form of an integrated legal regime rather than a set of isolated norms. For Ukraine, this poses a particular challenge, as national legislation remains largely sector-based, whereas future regulatory models are inherently interdisciplinary.

5. Conclusion

The article demonstrates that digital technologies are no longer merely auxiliary instruments of corporate governance or voluntary elements of corporate social

responsibility. They are progressively transforming into structural components of contemporary legal regulation, shaping the content, modes of implementation, and enforcement mechanisms of obligations in the fields of sustainable development, human rights protection, environmental governance, and corporate accountability.

A key result of the study lies in substantiating that digital mechanisms, including algorithmic audits, digital ESG reporting systems, blockchain-based traceability tools, IoT based solutions, and platform accountability regimes, exhibit a dual legal nature. On the one hand, they operate as technological infrastructures; on the other hand, they function as normatively relevant elements of legal compliance, increasingly embedded in binding regulatory frameworks. This duality challenges the traditional distinction between “hard law” and ostensibly “soft” technological practices and necessitates a reconsideration of the role of digital instruments within the legal model of socially responsible business conduct. The article further demonstrates that EU legal regulation reflects a qualitative shift in regulatory technique. Rather than relying primarily on ex post control and documentary verification, growing importance is attached to the embedding of legal requirements directly into digital systems. Through instruments such as the CSRD, CSDDD, the AI Act, and the DSA, legal obligations are operationalised by means of continuous data collection, automated monitoring, algorithmic risk management, and mandatory auditing procedures.

In the context of Ukraine’s post-war recovery, the article demonstrates that digital accountability mechanisms should be understood as system-forming elements of the legal architecture of reconstruction, rather than merely as technical tools of corporate governance or instruments of regulatory alignment. Under conditions of large-scale reconstruction, international assistance, and heightened institutional vulnerability, digital ESG reporting, algorithmic audits, and blockchain-based traceability function as legally significant safeguards ensuring transparency, traceability, and enforceability of sustainability, human rights, and environmental obligations. By embedding EU legal standards directly into digital infrastructures, these mechanisms transform post-war recovery from a politically declared objective into a legally reviewable and institutionally controllable process, mitigating corruption and misallocation risks and creating a structural bridge between reconstruction and European integration.

The article develops this argument through several interrelated analytical contributions. First, the article conceptualises digital mechanisms of socially responsible business conduct as an autonomous analytical category of legal regulation, rather than as a set of auxiliary managerial or technological tools. In contrast to fragmented approaches focusing separately on ESG reporting, due diligence platforms, or algorithmic audits, the study proposes a coherent legal model integrating these instruments within a unified regulatory logic of sustainable development and corporate accountability. Second, the article demonstrates that digitalisation transforms the functional structure of legal responsibility, shifting it from reactive enforcement towards preventive, continuous, and evidence-oriented regulation. Digital mechanisms are shown to perform preventive, supervisory, and evidentiary functions with direct legal relevance, thereby expanding the doctrinal understanding of responsibility in contemporary economic law. Third, the study offers a functional legal interpretation of algorithmic audits and digital ESG infrastructures as functionally institutionalised forms of external control. Algorithmic audits under the AI Act and the Digital Services Act are analysed as legally significant procedures generating

binding expectations, regulatory oversight, and potential liability, contributing to the development of the law-and-technology discourse on algorithmic accountability. Finally, the article provides a legal analysis of the Ukrainian regulatory context, identifying both existing digital institutional preconditions and systemic gaps in the regulation of socially responsible business. The novelty of this perspective lies in linking digital accountability mechanisms with European integration and post-war reconstruction, where transparency, traceability, and accountability acquire heightened normative significance.

From a theoretical perspective, the findings of the study confirm that contemporary economic and corporate law is evolving towards a model in which legal norms are increasingly embedded in technological systems. This development necessitates a rethinking of traditional understandings of compliance, control, and proof, as adherence to legal requirements is progressively demonstrated through the participation of economic actors in digital systems of monitoring and behavioural recording. From a regulatory perspective, the study shows that effective governance of socially responsible business depends not only on substantive legal standards, but also on the existence of a robust digital infrastructure capable of ensuring their practical implementation. The experience of the European Union demonstrates that sustainability regulation without digitalisation risks remaining largely declaratory, while digitalisation without appropriate legal framing may undermine accountability and lead to infringements of fundamental rights.

For Ukraine, the results of the study point to the need to move beyond fragmented digital initiatives towards the development of a coherent national model of digital governance of socially responsible business, aligned with EU law. This includes, in particular, the institutionalisation of digital ESG reporting, the phased introduction of due diligence regimes supported by digital tools, and the articulation of principles of algorithmic accountability in economically sensitive sectors. Future research may focus on the empirical assessment of the effectiveness of specific digital mechanisms, the analysis of judicial practice concerning digital evidence in sustainability-related disputes, or the examination of interactions between digital accountability tools and financial regulation. At the same time, the present article establishes a foundational legal model for understanding digital mechanisms as system-forming elements of the regulation of socially responsible business, rather than as merely auxiliary innovations.

References

- Abdallah-Ou-Moussa, S., Wynn, M., Kharbouch, O., & Rouaine, Z. (2024). *Digitalization and corporate social responsibility: A case study of the Moroccan auto insurance sector*. *Administrative Sciences*, 14(11), Article 282. <https://doi.org/10.3390/admsci14110282>
- Ajakwe, I. U., Ajakwe, S. O., Lee, J. M., & Kim, D. S. (2025). *Internet-of-things–blockchain integration in environmental pollution monitoring data management: Trends and techniques*. *International Journal of Environmental Science and Technology*, 22, 16123–16142. <https://doi.org/10.1007/s13762-025-06615-x>
- BDO in Ukraine. (n.d.). *CSRD and why it is important for business in Ukraine*. European Business Association. Retrieved from <https://eba.com.ua/en/bdo-v-ukrayina-pro-csrd-i-tse-vonavazhlyvo-dlya-biznesu-v-ukrayini>
- Cabinet of Ministers of Ukraine. (2024). *On approval of the Strategy for the introduction of sustainability reporting by enterprises (Order No. 1015-r of October 18, 2024)*. Retrieved from <https://zakon.rada.gov.ua/laws/show/1015-2024-%D1%80#Text>

- Caplan, R., Donovan, J., Hanson, L., & Matthews, J. (2018). *Algorithmic accountability: A primer*. Data & Society Research Institute. Retrieved from https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf
- Council of the European Union. (2024, May 21). *Artificial intelligence (AI) Act: Council gives final green light to the first worldwide rules on AI*. Retrieved from <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai>
- Debevoise & Plimpton LLP. (2023). *The extra-territorial impact of the Corporate Sustainability Reporting Directive- Broadening the scope of sustainability reporting to worldwide groups*. Retrieved from <https://www.debevoise.com/insights/publications/2023/11/the-extra-territorial-impact-of-the-corporate>
- EcoVadis. (n.d.). Global sustainability, one platform. Retrieved from <https://ecovadis.com/>
- European Commission. (n.d.). *DSA: Very large online platforms and search engines*. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>
- European Commission. (n.d.). *Supervision of the designated very large online platforms and search engines under the Digital Services Act*. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>
- European Law Institute. (2022). *ELI principles on blockchain technology, smart contracts and consumer protection*. Retrieved from https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection.pdf
- European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2464 on corporate sustainability reporting*. Retrieved from <https://eur-lex.europa.eu/eli/dir/2022/2464/oj/eng>
- European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2022/858/oj>
- European Parliament & Council of the European Union. (2022a). *Regulation (EU) 2022/2065 (Digital Services Act)*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065>
- European Parliament & Council of the European Union. (2023). *Regulation (EU) 2023/1542*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2023/1542/oj>
- Goodman, E., & Trehu, J. (2023). *Algorithmic auditing: Chasing AI accountability*. *Santa Clara High Technology Law Journal*, 39(3), Article 1. Retrieved from <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1689&context=chtlj>
- Government of France. (2017). *Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*. Retrieved from <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034290626/>
- Government of Germany. (2021). *Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (Lieferkettensorgfaltspflichtengesetz – LkSG)*. Retrieved from <https://www.gesetze-im-internet.de/lksg/BjNR295910021.html>
- ISPnext. (n.d.). *ISPnext & IntegrityNext: Working together to build a sustainable and transparent supply chain*. Retrieved from <https://www.ispnext.com/en/partner-page-integritynext>
- Jinyoung, H. (2024). *Corporate social responsibility (CSR) in the digital age: Investigating the challenges and future insights*. *GSC Advanced Research and Reviews*, 21(1), 503–518. <https://doi.org/10.30574/gscarr.2024.21.1.0383>
- Legal 500. (n.d.). *Public procurement in Ukraine: Strategic guide for international suppliers*. Retrieved from <https://www.legal500.com/developments/thought-leadership/public-procurement-in-ukraine-strategic-guide-for-international-suppliers>
- Markle, A. (n.d.). *Early impacts of public beneficial ownership registers: Ukraine*. OpenOwnership. Retrieved from <https://www.openownership.org/en/publications/early-impacts-of-public-beneficial-ownership-registers-ukraine>

- Martín-Baos, J. Á., Rodríguez-Benitez, L., García-Ródenas, R., & Liu, J. (2022). *IoT-based monitoring of air quality and traffic using regression analysis*. Applied Soft Computing, 115, Article 108282. <https://doi.org/10.1016/j.asoc.2021.108282>
- MediaLaws. (n.d.). *Auditing platforms under the Digital Services Act*. Retrieved from <https://www.medialaws.eu/auditing-platforms-under-the-digital-services-act>
- Meena, K., Mayuri, A. V. R., Preetha, V., & Krishna Veni, N. N. (2022). *5G narrowband IoT-based air contamination prediction using recurrent neural network*. Sustainable Computing: Informatics and Systems, 33, Article 100619. <https://doi.org/10.1016/j.suscom.2021.100619>
- Merlo, A., Mendonça, D., Santos, J., Carvalho, S., Guerra, R., & Brandão, D. (2025). *Blockchain for the carbon market: A literature review*. Discover Environment, 3, Article 68. <https://doi.org/10.1007/s44274-025-00260-4>
- Net Help. (2025, August 17). *LAAS, SAAS and PAAS: What they are, differences and examples*. Retrieved from https://ngo-it-help.org/2025/08/17/iaas_saas_paas/
- OECD (n.d.). *Responsible business conduct and technology*. Retrieved from <https://www.oecd.org/en/topics/sub-issues/due-diligence-guidance-for-responsible-business-conduct/responsible-business-conduct-and-technology.html>
- OECD. (2023). *OECD guidelines for multinational enterprises on responsible business conduct*. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_a0b49990/81f92357-en.pdf
- Pérez, C., López, I., & López, F. (2025). *Blockchain-based evidence and legal validity: Reformulating norms for decentralized justice systems*. Rechtsnormen Journal of Law, 3(2), 180–189. Retrieved from <https://www.researchgate.net/publication/391130263>
- Ramadan, M. N., Ali, M. A., Khoo, S. Y., Alkhedher, M., & Alherbawi, M. (2024). *Real-time IoT-powered AI system for monitoring and forecasting of air pollution in industrial environment*. Ecotoxicology and Environmental Safety, 283, Article 116856. <https://doi.org/10.1016/j.ecoenv.2024.116856>
- Soori, M., Karimi Ghaleh Jough, F., Dastres, R., & Arezoo, B. (2024). *Blockchains for industrial Internet of Things in sustainable supply chain management of Industry 4.0: A review*. Sustainable Manufacturing and Service Economics, 3, 100026. <https://doi.org/10.1016/j.smse.2024.100026>
- Swart, C., & Zincume, P. (2025). *ESG reporting and digitalization in financial services: A scoping review of emerging trends and gaps*. In Proceedings of the IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). <https://doi.org/10.1109/ICE/ITMC65658.2025.11106614>
- Taylor Wessing. (2021). *Leitfaden zum Lieferkettensorgfaltspflichtengesetz*. Retrieved from <https://www.taylorwessing.com/-/media/taylorwessing/files/germany/2021/07/tw2021leitfaden-zum-lieferkettensorgfaltspflichtengesetzesstand-30072021.pdf>
- Veale, M., & Zuiderveen Borgesius, F. (2021). *Demystifying the draft EU Artificial Intelligence Act*. Computer Law Review International, 22(4), 97–112. Retrieved from <https://ssrn.com/abstract=3896852>
- Verkhovna Rada of Ukraine. (2010). *Law of Ukraine “On Personal Data Protection”*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
- Verkhovna Rada of Ukraine. (2020). *Law of Ukraine “On Electronic Communications”*. Retrieved from <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
- White & Case. (2024). *Time to get to know your supply chain: EU adopts Corporate Sustainability Due Diligence Directive*. Retrieved from <https://www.whitecase.com/insight-alert/time-get-know-your-supply-chain-eu-adopts-corporate-sustainability-due-diligence>
- World Economic Forum. (2020). *Redesigning trust: Blockchain for supply chains*. Retrieved from https://www3.weforum.org/docs/WEF_CAIR_Case_Study_Blockchain_for_Supply_Chains_2020.pdf
- Zheng, L. J., Zhang, J. Z., Au, A. K. M., Wang, H., & Yang, Y. (2023). *Leveraging technology-driven applications to promote sustainability in the shipping industry: The impact of digitalization on corporate social responsibility*. Transportation Research Part E: Logistics and Transportation Review, 176, Article 103201. <https://doi.org/10.1016/j.tre.2023.103201>