The Future of Corporate Liability: Why the 'Failure to Prevent' Model Matters for Human Rights Due Diligence Regulation

Dr Irene Pietropaoli **Giuseppe Di Vetta**

The 'failure to prevent' model is a legal construct under which a corporate entity can be held strictly liable for failing to prevent certain unlawful acts (typically committed by associated persons), unless it can prove that it had adequate procedures in place to prevent them. It shifts the legal burden onto the company to demonstrate that it took all reasonable steps to prevent the misconduct, rather than requiring prosecutors to prove corporate intent or direct involvement. Examples of this model are the UK criminal offences for failure to prevent bribery (Bribery Act 2010, s. 7), failure to prevent facilitation of tax evasion (Criminal Finances Act 2017, ss. 45-46) and failure to prevent fraud (Economic Crime and Corporate Transparency Act 2023, which will come into force in September 2025). The 'failure to prevent' model offers a framework for attributing liability to companies in cases of adverse human rights or environmental impacts linked to their global operations and supply chains. It can provide a regulatory model under the evolving landscape of human rights due diligence (HRDD) legislation and the revision to the Corporate Sustainability Due Diligence Directive (CSDDD) liability regime introduced by the Omnibus Package. This model shifts the focus from tracing individual perpetrators within corporate structures to assessing whether the organisation exercised due diligence to prevent foreseeable harms through effective risk management and governance. It aligns with the risk-based and preventative nature of the UN Guiding Principles on Business and Human Rights and the CSDDD and responds to enforcement challenges in transnational corporate networks. As this blog explains, the 'failure to prevent' model offers legal coherence, practical enforceability, and alignment with broader legislative trends in Europe, while promoting corporate accountability without relying on reconstructing individual fault or intent.

A key revision contemplated within the Omnibus Package concerning the Corporate Sustainability Due Diligence Directive (CSDDD) involves the proposed elimination of the EU-wide civil liability regime. This regime, as originally conceived, provided a mechanism for seeking redress for damages stemming from the business activities of companies found to be in violation of the CSDD's stipulated requirements. Originally, the harmonized European civil liability regime was intended to serve as a crucial mechanism for enforcing the due diligence obligations outlined within the directive. Its objective was to guarantee victims access to effective remedies by extending statutes of limitations and establishing a standardized procedural framework applicable across all Member States.

The directive's enforcement relies on a tripartite mechanism. First, Member States are required to establish an autonomous and independent supervisory authority for verifying corporate compliance to the directive, with particular emphasis on due diligence obligations. This supervisory mandate encompasses the authority to conduct inspections, request information (disclosure), and undertake investigatory activities. Furthermore, the designated authority should be empowered to mandate that non-compliant companies implement interim measures to forestall irreparable harm resulting from adverse impact risks that the company should have prevented through the exercise of due diligence. A further mechanism for enforcement entails the imposition of civil liability for damages arising from the failure to prevent adverse impacts. The Omnibus Package proposes to curtail the scope of this mechanism by fully eliminating the harmonized European civil liability regime previously established under the directive, as detailed in the version approved in July 2024.

The final mechanism, characterized by its public nature, primarily aims to serve as a deterrent. Specifically, Article 27 of the directive mandates that Member States implement a defined system of sanctions, encompassing pecuniary penalties, applicable to cases where national law provisions transposing the directive are infringed. Aligning with approaches adopted in other sectors, the directive generally stipulates that sanctions must be effective, proportionate, and dissuasive. While Member States retain discretion in determining the specific types of sanctions to be applied, the directive mandates the inclusion of pecuniary penalties in all cases. Article 27(4) further requires Member States to consider a range of criteria

when establishing both the applicability and the level of sanctions for breaches of the obligations outlined in the directive. The criteria articulated in paragraph 4 underscore the punitive character of the sanctions that Member States are required to adopt during the transposition process. The public sanctioning regime, as defined by the directive, undeniably aims to deter non-compliance; moreover, the potential level of sanctions may be substantial. In light of these considerations, and irrespective of their classification under domestic law, the sanctions intended to implement the directive within national legal systems are considered to fall under criminal law domain 'within the meaning of the Convention' according to the European Court of Human Rights' case-law.

Article 27 also outlines a specific criterion for determining the amount of pecuniary penalties: the directive establishes a maximum 'cap', stipulating that the sanctions must not be less than 5% of the company's worldwide net turnover. This provision is subject to modification under the Omnibus Package, which proposes the elimination of the 'cap', thereby tasking the Commission with developing guidelines to ascertain the appropriate level of pecuniary sanctions in a manner aligned with the parameters outlined in Article 27(4).

Following the proposed elimination of the EU-wide civil liability regime, the directive's enforcement may become primarily contingent upon public mechanisms, particularly punitive sanctions. The directive grants Member States discretion in defining numerous key aspects of the public sanctioning regime. However, one element remains unequivocal: it establishes a corporate liability regime, specifically targeting those companies that have failed to comply with the obligations established by the directive as transposed into national law. Member States retain a degree of discretion in determining the precise interpretation of 'infringement' and the corresponding preconditions for liability.

The European directive aligns with a broader legislative trend, exemplified by countries that have already enacted (or are in the process of enacting) laws imposing human rights due diligence obligations on companies (HRDD Laws). These laws aim to prevent violations of human rights and environmental values, extending beyond the scope of their direct operations to encompass the entire value chain. Notable examples of this trend include the French Loi Vigilance and the German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz - LkSG). HRDD laws impose punitive sanctions on companies that fail to adequately prevent the risk of human rights abuses or other adverse environmental impacts.

Within the framework of mandatory due diligence law, companies are held liable for inadequately performing the due diligence process, thereby failing to prevent the risk of adverse impacts. Literature identifies the 'failure to prevent' as the dominant paradigm for delineating corporate criminal liability under such legislation. The 'failure-to-prevent' model also serves as a key reference point for the CSDDD, which Member States should consider when formulating the corporate liability regime transposing the directive.

The 'failure to prevent' model offers a suitable framework for establishing corporate (criminal) liability in the context of implementing due diligence obligations. It places liability within the organization itself, particularly in its capacity to effectively manage risks associated with its operations and supply chains. Due diligence, as widely understood, constitutes an iterative process through which companies identify and evaluate risks inherent in their activities and those of their subsidiaries and business partners. The 'failure to prevent' paradigm grounds corporate liability specifically in the omission or inadequacy of this due diligence process. Aligned with a risk-based regulatory approach, this model of corporate criminal liability operationalizes polycentric governance scheme, wherein due diligence assumes a critical function.

This model of corporate liability has seen increasing adoption as a technical solution to enhance the accountability of corporate actors operating within complex environments, such as global value chains. The 'failure to prevent' approach is clearly differentiated from nominalist corporate criminal liability models, which rely on the principle of identification, and further diverges from models predicated on organizational fault. In contrast to derivative or nominalist models, the 'failure to prevent' approach typically obviates the need for ascertainment of the principal offense and the identification of the natural person who perpetrated it in the company's interest. Consequently, corporate liability under this model does not necessitate the reconstruction of individual decision-making processes within the corporate environment. Therefore, it represents a particularly suitable framework for application within corporate groups and, especially, corporate networks such as global supply chains. In these contexts, reconstructing decision-making processes proves infeasible, and the precise identification of the natural persons acting in the entity's interest presents significant challenges. According to the 'failure to prevent' paradigm, the salient factor is the company's exercise of its relative organizational power (value chain management) to mitigate the risk of human rights violations or other adverse impacts within the scope of its operations and chain of activities. The scope of what a company can reasonably be expected to do is contingent upon the organizational and cognitive resources it can deploy, the specific circumstances involved, its effective power of leverage, and its position within the value chain. Thus, the 'failure-to-prevent' approach exhibits sensitivity to the concrete organizational and corporate environment.

The failure to prevent is close to the models of criminal liability of companies based on organizational fault. However, compared to them, it realizes a significant simplification, especially under the profile of the connection that must exist between the adverse event, such as the violation of a human right, and the organizational conduct of the company. Based on the failure to prevent, the establishment of a causality in the strict sense is not required - the company is liable when it has not adopted adequate compliance to prevent the risk of a specific category of adverse impacts, in the context of reference. In this perspective, it is possible to draw a significant distinction between the models that associate the company's liability with the causation of the actual adverse impact and those that instead require the company to prevent it, adopting appropriate measures and procedures.

Furthermore, the model can ensure the effectiveness of the public enforcement regime of the CSDDD, given its consistency with the transnational scope of the due diligence obligations outlined by the directive. Section 7 of the UK Bribery Act 2010 introduced an early example of the 'failure to prevent' model, holding companies criminally liable for failing to prevent bribery by associated persons unless they can demonstrate having 'adequate procedures' in place to prevent such conduct. This approach provides enforcement authorities with a clear pathway to prosecute corporate wrongdoing without the need to establish the liability of specific individuals. As evidenced by the experience of the UK Bribery Act, the 'failure to prevent' model applies on the basis of a territorial approach to jurisdiction, albeit one that may be highly advanced (territorial extension; corporate objective territoriality). Thus, while the application of domestic law is typically insulated from jurisdictional conflicts, the due diligence obligations of companies are designed to extend beyond the boundaries of the home country's jurisdiction to encompass subsidiaries and business partners operating in foreign jurisdictions. In this manner, the spillover effect intended by the directive is achieved.

The 'failure to prevent' model represents a shift in how corporate liability is conceptualised and enforced. By anchoring accountability in a company's preventative systems and organisational capacity to manage risk, it moves beyond traditional liability models that require proof of individual wrongdoing. Its compatibility with complex corporate structures and global supply chains makes it a particularly apt mechanism for enforcing HRDD obligations in the CSDDD and related legislation.

Authors:

Giuseppe Di Vetta, Assistant Professor, Scuola Superiore Sant'Anna
Dr Irene Pietropaoli, Senior Fellow in Business and Human Rights, BIICL

URL: https://www.biicl.org/blog/114/the-future-of-corporate-liability-why-the-failure-to-prevent-model-matters-for-human-rights-due-diligence-regulation

© 2026 BIICL | A company limited by guarantee | Registered in England No. 615025 | Registered Charity No. 209425