SRE in the Law of Technological Risk: Reliability and responsibility

Author:
Torres Ponce, Mariano Enrique
Lawyer specialized in Computer Law

ABSTRACT

This paper argues that effective oversight of modern digital systems requires more than legal knowledge. Regulators need working fluency in code, systems, data pipelines, and the behavior of algorithms in production. Document review on its own no longer reveals how decisions are made or where risks arise. The paper outlines a practical capability model built around technical literacy, data governance and lineage, risk-based auditing, socio-technical impact assessment, and close collaboration with engineering teams. The model is grounded in current practice: European initiatives that train specialists in algorithmic audits and AI impact assessments, Singapore's 2020 Model AI Governance Framework with its emphasis on risk-proportionate controls, and Latin American approaches that draw on flexible administrative traditions to make steady progress. These lessons are translated into concrete tools for agencies, including inspection protocols, evidence standards for logs and metrics, test sandboxes, and red team exercises. The paper closes with training pathways and institutional options that help scale these skills while preserving due process and room for innovation.

KEYWORDS

Algorithmic governance; Regulatory capacity; Algorithmic audits; AI impact assessments; Risk-based supervision; Technical literacy for regulators; Data governance and lineage; Evidence standards for logs and metrics; Testing sandboxes; Red team exercises; Public sector oversight; Socio-technical risk.

EXECUTIVE SUMMARY

Background: Legal oversight of digital systems increasingly requires technical fluency. Understanding how risks arise and how decisions are made takes more than reviewing documents. It also calls for familiarity with code, infrastructure, data flows, and the behavior of algorithms in production environments.

Gap: Existing regulatory approaches often rely on policy statements and ex-post evaluations, with limited access to replicable technical evidence. Capabilities such as risk-based algorithmic audits, end-to-end data lineage, and standardized evidence protocols for logs and metrics remain underdeveloped across public agencies.

Purpose: This paper proposes a capability model for regulators that integrates legal judgment with technical literacy and proportional supervision. It translates emerging international practices into operational tools that agencies can begin to adopt.

Methodology: The analysis draws on recent regulatory initiatives, including Europe's proposal for the Artificial Intelligence Act, Singapore's 2020 Model AI Governance Framework, and Latin American approaches rooted in flexible administrative traditions. These are synthesized into actionable mechanisms that support oversight without stifling innovation.

Results: Five core capabilities are identified: literacy in code and systems; governance and lineage for data; risk-based auditing; socio-technical impact assessment; and structured collaboration with engineering teams. The model includes instruments such as inspection protocols, standards for logs and metrics, controlled testing environments, and adversarial simulation exercises.

Conclusion: Effective supervision of automated systems requires hybrid expertise and institutional design that supports continuous learning. With targeted training and clear procedural tools, regulators can build trust, preserve due process, and foster responsible innovation.

TABLE OF CONTENTS

A. INTRODUCTION

Debates on technological reliability and legal responsibility have reached a point where old assumptions about risk in automated, high-stakes systems can no longer stand. Operating digital infrastructures built on automation, orchestration, and continuous delivery no longer treats error as a rare anomaly. It treats error as an inherent feature of complex services that must be measured, bounded, and used to drive organizational learning. This shift turns attention from chasing perfect systems to building ones that can bounce back from errors. It opens a vital conversation between engineers and legal experts, not just in Latin America, where debates on algorithmic harm emphasize proactive safeguards, but also in places like the United States, where NIST's AI Risk Management Framework (AI RMF 1.0, 2023) calls for measurable risk controls in automated systems. This dialogue links technical practices with legal duties of foresight, traceability, and response across diverse regions (de Teffé & Medon, 2020).

What some scholars describe as a law of technological risk can be read as a response to distributed agency in systems where humans, software, and platforms act together. Attribution stops being a purely causal exercise and becomes an institutional reconstruction of design choices, oversight routines, and controls across the service life cycle. Regional developments in data protection and civil liability helped anchor this transition by articulating duties of governance, ex-ante approaches to risk, and workable connections between information, security, and redress. Latin American scholarship on personal data has consistently shown that prevention and responsibility rest on objective organizational duties and user protection criteria, which aligns well with technical practices of observability and post-incident learning (Bioni & Dias, 2020).

The platform ecosystem adds further complexity because it mediates content flows, automated decisions, and the delivery of critical services. Regional work on intermediary liability has pointed to the need for differentiated standards that track functions, risk exposure, and real capacities for control, with attention to notice regimes, traceability, and proportionate response. That body of doctrine offers a useful toolkit to understand reliability as an institutional duty rather than a mere technical expectation of performance, which directly affects how negligence should be defined in automated environments (Palazzi, 2012).

The goal here is to clarify how a culture of operational reliability reshapes the legal semantics of failure and negligence, and to what extent it can ground a verifiable standard of reasonable technical care. The argument assumes that reliability means building organizational capabilities to anticipate, absorb, and learn from incidents through metrics, documentation, and institutional memory. The discussion is framed within a Latin American horizon that has already developed criteria on privacy, risk moderation, and user protection, with clear potential to project a theory of responsibility for automated systems that recognizes the inevitability of error without relaxing the duty of care. The key is to connect legal prevention with technical risk management so that error ceases to signal blame and becomes usable input for improvement within traceable and auditable governance structures (de Teffé & Bodin de Moraes, 2017).

B. THE SRE PARADIGM AND THE CULTURE OF RELIABILITY

SRE was born to make complexity governable, yet its strength lies less in tooling than in how it organizes responsibility. When a team adopts metrics that track what truly matters for users, records explicit service thresholds, and accepts a bounded margin for error, it builds a common language across development, operations, and management. That shared language makes room for decisions without dramatizing failure and without clinging to the illusion of total control. In practice, the cultural shift begins when an organization stops debating whether failure is allowed and starts asking what evidence it needs to move fast without breaking what is essential. Reliability is not a promise; it is something you can show.

An error budget operates most effectively as an operational agreement that sets clear priorities and prevents unchecked momentum. Rather than permitting recklessness, it requires robust justification for changes when a service approaches its limits. However, this agreement holds only if the metrics genuinely reflect users' actual experiences, not merely what suits the technical team. Poorly chosen indicators can create a misleading sense of security while risks accumulate unnoticed. Latin American scholarship on decision technologies emphasizes the need to regularly reassess measurement assumptions and biases, as a system chasing hollow numbers is no safer than one without metrics at all; it simply becomes harder for overseers and those accountable in legal contexts to see its flaws (Melo, 2022; de Teffé & Medon, 2020).

Blameless post-incident reviews are sometimes presented as a cultural gesture, although their real value is institutional. Taken seriously, they become a memory device that converts discrete errors into structural improvements. When they trace the causal arc with sufficient clarity, surface the technical hypotheses that failed, and leave auditable footprints of the remediation decisions, they turn into evidence of due care. Responsibility no longer rests on heroic narratives and instead anchors in a choreography of design, monitoring, and correction that can be examined with rigor. This sits well with regional approaches that tie responsibility to organizational duties of prevention, transparency, and continuous response rather than to the mere absence of incidents over a period of time (Doneda, Mendes, & de Souza, 2020; Bioni & Dias, 2020).

For SRE to carry normative weight, a modest threshold should be available on demand without special preparation. A service ought to show a map of critical indicators aligned to user outcomes, visible and agreed thresholds, alert rules that trigger human intervention, a recent history of error-budget consumption, and a repository of post-incident reviews with improvements that actually made it into production. This does not exhaust the practice, but it separates the rhetoric of reliability from its exercise in the real world. Where these elements are missing or cannot be produced easily, SRE remains discourse rather than structure. In Latin American contexts, where data governance and user protection frameworks push toward objective organizational duties, that kind of technical transparency aligns with legal expectations of traceability and with a notion of reasonable care that is proved by procedures rather than intentions (Bioni & Dias, 2020).

There is a common pitfall worth naming. Some organizations adopt SRE vocabulary without changing their power dynamics and end up using indicators as political shields. Risk does not shrink with more dashboards if the difficult conversation about priorities never happens. The practice grows sturdy when metrics carry real consequences, for example by halting deployments when the error budget is depleted or by postponing shiny features to reinforce recovery mechanisms. Costly choices like these are where culture becomes tangible and where the law can recognize a form of technical diligence that is not decorative but effective. Experience in observability and operational risk across the region leaves a clear lesson that is both simple and demanding. Transparency without the capacity to respond is an illusion. Capacity to respond without learning is a treadmill. The combination of both is sustained reliability.

Perhaps the most meaningful contribution SRE offers to legal debate is a shift from blame to architectures of care. It absolves no one for failing. It requires proof that the system was prepared to fail in a contained and recoverable way. Under that lens, negligence stops being confused with error and is defined instead by the absence of structure to detect issues in time, understand them with evidence, and correct them in a stable manner. This inversion brings technical practice closer to Latin American frameworks that conceive responsibility as a task of ongoing governance, where prevention and repair belong to the same cycle and where diligence is verified in documents, traces, and living processes rather than in performative claims about quality (de Teffé & Medon, 2020).

C. LAW OF TECHNOLOGICAL RISK AND RESPONSIBILITY IN AUTOMATED ENVIRONMENTS

Legal systems often lag behind technology, especially when algorithms learn, adapt, and make decisions while laws still focus on human actions and clear-cut events. This mismatch creates a challenge: traditional ideas of authorship, cause, and blame struggle to address the complexities of modern systems. What we need is a new approach to technological risk, not as a standalone legal field but as a practical way to manage uncertainty rather than eliminate it. For instance, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) pushes organizations to protect users from automated decisions, while Europe's General Data Protection Regulation (GDPR) demands clear accountability for algorithmic choices. These examples show how global legal frameworks are starting to grapple with the same challenges (de Teffé & Medon, 2020).

In this setting, risk stops being a contingent threat and becomes part of the normal operation of a digital society. The question is no longer whether failures will occur but how their effects are allocated, who anticipates them, and who bears the costs when systems do not behave as expected. That conceptual move brings law closer to contemporary engineering, which already treats error as inevitable and builds mechanisms to absorb it without collapse. What changes is the measure of diligence. Instead of counting the absence of failures, diligence is assessed by an institution's capacity to prevent, detect, and respond in time. This logic aligns with an ex-ante

understanding of responsibility in which the primary duty is not to avoid all harm but to show that risk was managed reasonably (de Teffé & Medon, 2020).

A key step in this transition is the shift from individual fault to institutional responsibility. Automated systems are collective products in which designers, operators, infrastructure providers, and algorithms act together. Isolating a single culprit is as unhelpful as it is unfair. Attribution therefore centers on governance structures, on the presence of control policies, documented decisions, data traceability, and effective correction mechanisms. That structure sets a new standard of technical care, analogous to what SRE calls a culture of reliability. In both domains responsibility is proven by how care is organized, not by a promise of perfect results. The parallel suggests that law can learn from engineering less in its tools than in its readiness to treat error as constitutive of order (Doneda, Mendes, & de Souza, 2020).

Latin American scholars highlight how automation can deepen structural inequalities, emphasizing the need for fair risk management. This insight isn't unique to the region. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) underscores robust data safeguards to protect users from automated decisions. Similarly, Europe's General Data Protection Regulation (GDPR) sets strict standards for algorithmic accountability. These frameworks show that risks often hit hardest where protections are weakest, calling for a law of technological risk that prioritizes both efficiency and justice across borders (Melo, 2022; Bioni & Dias, 2020).

The hard legal problem is turning that idea of governance into enforceable rules. Experience shows that purely declarative models, whether codes of conduct, ethical principles, or technical guidelines, have little effect unless they are tied to concrete mechanisms for auditing and accountability. Several jurisdictions have started to test this translation through algorithmic impact-assessments and documentation duties as conditions to operate automated systems in regulated sectors. The trend signals a change in logic. Compliance is measured by the ability to show processes and not only outcomes. In that sense, a law of technological risk increasingly resembles a law of institutional reliability, where responsibility is attributed not only for damage but for the lack of structure to prevent or manage it.

This framework does not displace classical models of liability; it complicates them. Fault still matters, although its meaning shifts. It is no longer just the careless conduct of an

individual. It can be the inertia of an organization that lacks adequate policies to anticipate and correct errors. Negligence may present as missing documentation, absent supervision, or resistance to learning from incidents. If it consolidates, a law of technological risk will offer a shared language for engineers and jurists, one that lets us discuss care and error without moralism or technocracy and that treats reliability not as a technical privilege but as a contemporary form of social responsibility.

D. REDEFINING "FAILURE" AND "NEGLIGENCE" THROUGH THE SRE LENS

In Site Reliability Engineering, talking about failure means finding ways to grow stronger. Complex systems don't treat errors as rare breakdowns or chaos. They're just part of how things work. For example, when a streaming service faces a sudden spike in users, its automated scaling might stumble if a server configuration isn't ready. Chasing perfection in such dynamic setups, with constantly shifting components and unpredictable user actions, isn't realistic. Mistakes are the cost of innovation. The real test is how teams handle them, like setting up alerts to catch issues early or running drills to practice recovery.

Good governance turns a system failure into a chance to improve, not a legal problem. A company shows strength by being ready to handle errors. For example, logging a payment system glitch and analyzing its cause quickly can prevent bigger issues. But if the same glitch keeps happening without fixes, that's a clear sign of carelessness. Proactive steps, like updating system checks after an incident, are key to responsible tech oversight (Kubo, 2022).

SRE offers a smart way to manage risk. The error budget sets a clear limit on acceptable downtime, keeping services reliable without stopping progress. It's not about being careless; it's a safety net that lets teams innovate but pauses updates if risks grow too big. For example, a team might use logs to show they delayed a software update to stabilize a payment system. Legally, this makes abstract duties concrete, proving risks were tracked and managed. This approach shifts focus from blaming individuals to improving system design, aligning with ideas that prioritize prevention over punishment (Calo, 2021).

This perspective redefines negligence. It's not just about someone slipping up. It's about a company failing to set up ways to spot, track, and fix issues. For instance, if a delivery app keeps losing orders because it skips reviewing error logs, that's neglect. The real issue isn't the first mistake but refusing to learn from it. What used to be pinned on individuals

now hinges on system design and management. This aligns with ideas that stress accountability through better governance, not just pointing fingers (Smuha, 2020).

SRE's blameless post-incident reviews provide a fresh way to think about legal accountability. They accept that mistakes will happen but focus on how organizations respond as the real measure of responsibility. A solid review that digs into what went wrong, when it was caught, and how it was fixed can serve as evidence of careful management. Without such a record, it's easy to see neglect. Technical documentation, much like a legal record, captures the story of risk, ensures openness, and lets us judge decisions fairly. Though engineering and law speak different languages, they both strive to create trust through clear evidence.

The idea of controlled failure changes how we approach accountability in law. It's okay for systems to have some errors if they're planned for and kept under control. For instance, a banking app might briefly go offline during a software update, but that's different from crashing because no one tested the update first. The old mindset saw every mistake as a violation. Now, law should separate acceptable errors in complex systems from those showing carelessness or poor planning. The difference lies in preparation and response. It's not about excusing mistakes but about judging them based on how teams anticipate and handle them, like using real-time monitoring to spot issues or updating protocols after an outage.

This changes what we mean by reasonable technical care. It's not about ticking boxes on a fixed list but about committing to ongoing documentation, review, and improvement. Compliance isn't just about avoiding breakdowns. It's about showing a culture of reliability that proves every mistake leads to real progress. Engineering and law work together in a powerful way: technology provides the tools to track responsible practices, while law sets the expectation that those practices must be consistent and meaningful.

SRE offers a new way to approach risk. A failure doesn't automatically mean someone was careless. Instead, true diligence lies in how well an organization responds to problems, not just in the immediate result. By treating failures as opportunities to learn and negligence as a refusal to improve, we can clearly separate the two. This approach paves the way for a legal framework that embraces the complexity of technology and supports it with smart, responsive accountability.

E. REGULATORY IMPLICATIONS AND CHALLENGES FOR LAW

Automation and reliable systems push us to rethink regulation. Engineers know mistakes are part of the deal, but laws often act like everything can be perfectly controlled. For example, a self-driving car's software might misjudge a road signal, not because of bad coding but because real-world conditions are unpredictable. Instead of banning all errors, regulation should focus on spotting and fixing them fast. This means building systems to catch issues early, like automated alerts for software glitches, rather than setting rigid rules. Fields like aviation have long embraced this by designing backups that expect errors. Applying this to software, where problems spread instantly, is the new challenge (Smuha, 2020).

A reliability-focused approach puts the spotlight on how organizations learn, not just on avoiding mistakes. The real question is whether companies have systems to track errors and share what they find. For example, if a retail website crashes during a sale, a strong process might involve logging the issue and holding a team review to prevent repeats. This shifts responsibility from just following rules to being ready for problems. Law can learn from SRE's approach, which treats error management as a practical habit, not a reason to punish (Hood, Rothstein, & Baldwin, 2001).

Global practice is converging. In the European Union, DORA has been adopted for financial services and the proposed AI Act remains under negotiation. In the United States, NIST released the AI Risk Management Framework (AI RMF 1.0) in January 2023, providing a common structure for managing AI risk. In Asia, Singapore's 2020 Model AI Governance Framework promotes proactive, risk-based audits for automated systems, and similar debates are advancing in Japan and South Korea. Across Latin America, financial supervisors are updating digital-resilience playbooks and piloting process-based oversight. The common thread is a shift from one-time checks of finished products to continuous, transparent processes.

The challenge for law is keeping up with systems that learn from their mistakes. SRE's blameless reviews dig into what went wrong without pointing fingers. For example, if an e-commerce platform crashes during a sale, a good review might show the crash came from an overloaded server and suggest better load testing. This approach doesn't fit easily with legal traditions that see every error as a fault. Punishing every mistake, like in finance, can make companies hide problems, but rewarding openness through clear incident reports drives improvement (Smuha, 2020).

A law for managing tech risks can learn from SRE by balancing accountability with incentives to share mistakes. The point isn't to let errors slide but to turn them into lessons. For example, if a cloud service outage disrupts businesses, a detailed public report explaining the fix can do better than repeated fines for the same issue. Requiring transparent incident logs encourages companies to improve without fear of punishment (Hood, Rothstein, & Baldwin, 2001).

Regulating tech today goes beyond legal know-how. Regulators need to get comfortable with code, understand system setups, and follow how algorithms make decisions. Just checking paperwork won't cut it; they need to team up with engineers to turn technical data into real oversight. For example, auditing a chatbot's decision logs can reveal if it's misguiding users, leading to better safety checks. Europe is leading with training for algorithmic audits and AI reviews. In Asia, Singapore's 2020 framework pushes similar skills through risk-focused audits. Latin America's moving slower, but its flexible rules help it catch up (Doneda, Mendes, & de Souza, 2020).

Ethics cuts through the entire project. Accepting error as part of normal operation must not normalize harm. Controlled failure only makes sense where users enjoy effective safeguards and where tolerance stays within socially acceptable bounds. Regulation needs to strike a balance between flexibility and integrity. Excessive rigidity smothers innovation. Excessive permissiveness erodes trust. In that space law can redefine its role. Not as a brake on technique, but as a steward of public confidence. A culture of reliability understood as shared care, learning, and repair offers a conceptual bridge between the logic of systems and the logic of justice.

F. CONCLUSIONS

Technological reliability and legal responsibility now work hand in hand. Engineering keeps systems running, while law ensures they earn public trust. Both rely on building confidence among users. Site Reliability Engineering helps by using technical tools to make complex systems clear and answerable to scrutiny (NIST, 2023; European Commission, 2018).

This perspective is visible across jurisdictions. In the United States, NIST's AI Risk Management Framework (AI RMF 1.0, 2023) highlights the importance of measurable

controls. In Canada, PIPEDA sets clear requirements for consent, accountability, and safeguards. In Europe, the GDPR frames expectations for algorithmic accountability. In Asia, Singapore's 2020 Model AI Governance Framework encourages proactive, risk-based auditing. Taken together, these examples show that risk can be managed without pretending failure is impossible; the task is to learn from incidents through clear, well-structured processes (NIST, 2023; European Commission, 2018).

Thinking about responsibility through the lens of reliability changes the legal timeline. A model built primarily to repair harm struggles in environments where systems issue millions of automated micro-decisions every second. A posture of continuous observation, inspired by SRE, shifts attention to an organization's ability to detect, interpret, and respond. Under this view, diligence stops being a subjective ideal and becomes something you can evidence. Error budgets, service metrics, and post-incident reports read as documents of responsibility. They turn prudence into proof and make technical transparency the contemporary form of reasonable care.

This shift is not uniquely Latin American, although the region adds a necessary ethical emphasis. Societies marked by inequality feel the human cost of technical error more sharply and understand reliability as a matter of distributive justice. Globally, the same intuition is taking hold. The European Commission, NIST in the United States, and the OECD converge on risk-based approaches in which public trust stems from process transparency rather than formalistic box-ticking (NIST, 2023; OECD, 2019; European Commission, 2020). The implication is clear. The future of tech regulation will be shaped less by the volume of rules and more by the quality of the practices that sustain them.

Seen more broadly, a law of technological risk should not aim to discipline technique so much as to accompany its uncertainty. SRE shows that resilience emerges from cooperation among design, monitoring, and learning. Law can strengthen that cooperation by creating incentives for documentation, traceability, and transparent audit. The goal is not heavier control but a stronger institutional memory. An organization that preserves and analyzes its history of errors does more than show diligence. It builds a narrative of trust that law can recognize and protect.

The deepest regulatory innovation will be cultural. Accepting that systems fail does not normalize irresponsibility. It acknowledges the imperfect nature of all human and technical devices. Responsibility is no longer proven by the absence of error, but by the quality of

the response. A failure that is documented, reviewed, and corrected signals maturity. A repeated or denied error is the clearest evidence of negligence. A legal system able to tell them apart does not abandon sanction. It redirects it toward prevention and learning.

Global risk theory suggests that SRE offers a practical guide for this shift. It reframes the task: from fixing harm to building knowledge, from strict control to active monitoring, and from rigid rules to adaptable reliability. The real challenge is not whether law can match the pace of technology. It is whether law can adopt the same openness as engineering, recognizing that real care comes from learning from every mistake (Hood, Rothstein, & Baldwin, 2001).

G. REFERENCES

Beyer, B., Jones, C., Petoff, J., & Murphy, N. (2016). *Site reliability engineering: How Google runs production systems*. O'Reilly Media.

Bioni, B., & Dias, D. (2020). Responsabilidade civil na proteção de dados pessoais. *Civilistica.com, 9*(3), 1–23.

Calo, R. (2021). Liability for robots and other agents. *Annual Review of Law and Social Science, 17*, 105–123.

Cámara Nacional de Apelaciones en lo Civil, Sala D. (2018). *Asociación de Bancos de la República Argentina c/ IBM Argentina SA y otro s/ daños y perjuicios*. *La Ley Online*, AR/JUR/46837/2018.

de Teffé, C. S., & Bodin de Moraes, M. C. (2017). Redes sociais virtuais: Privacidade e responsabilidade civil. *Pensar, 22*(1), 108–146.

de Teffé, C. S., & Medon, F. (2020). Responsabilidade civil e regulação de novas tecnologias: Reflexões sobre a tomada de decisões com sistemas de inteligência artificial. *Revista de Estudos Institucionais, 6*(1), 151–182.

Doneda, D., Mendes, L. S., & de Souza, C. A. P. (2020). Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar, 23*(4), 1–20.

European Commission. (2018). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR)*. European Union.

European Commission. (2020). *Proposal for a regulation on digital operational resilience for the financial sector (DORA)*. European Union.

European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. European Union.

European Commission. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*. European Union.

Forsgren, N., Smith, D., Humble, J., & Frazelle, J. (2021). *Accelerate: State of DevOps 2021*. Google Cloud & DORA.

GitHub Engineering. (2018, October 30). October 21 post-incident analysis. *GitHub Blog.* https://github.blog/

Government of Canada. (2000). *Personal Information Protection and Electronic Documents Act (PIPEDA).* Justice Laws Website. https://laws-lois.justice.gc.ca/

Hood, C., Rothstein, H., & Baldwin, R. (2001). *The government of risk: Understanding risk regulation regimes.* Oxford University Press.

Infocomm Media Development Authority. (2020). *Model artificial intelligence governance framework* (2nd ed.). Singapore Government.

Kubo, M. (2022). Ethical and legal challenges in AI deployment: A Japanese perspective. *Journal of AI Ethics, 2*(3), 215–230.

Melo, B. L. D. A. A. (2022). Sistemas de inteligência artificial e responsabilidade civil: Dificuldades dos modelos tradicionais. *Revista de Direito da Faculdade de Jataí, 6*(1), 1–26.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* NIST.

Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on Artificial Intelligence.* OECD Publishing.

Palazzi, P. (2012). Responsabilidad de los intermediarios en Internet. *Revista de Derecho Privado y Comunitario, 2012*(1), 45–68.