SRE in the Law of Technological Risk: Reliability and responsibility

AUTHOR:
Torres Ponce, Mariano Enrique
Lawyer (LL.B.), Specialist in Computer Law

ABSTRACT

Oversight of digital infrastructures now requires a degree of operational awareness that traditional legal methods rarely anticipated. Modern systems change as they run, often through automated deployment pipelines or data-driven adaptations that are difficult to reconstruct after the fact. In learning models, internal decision paths may shift in ways that no occasional inspection can fully capture. A regulator who cannot follow at least part of this movement risks overlooking the very points at which routine disturbances turn into real harm.

This paper proposes a practical framework for supervision that treats technical literacy as part of the ordinary demands of public responsibility. The approach draws on regulatory experiences that have begun to incorporate algorithmic audits and impact assessments into everyday practice, on models that emphasise proportionality in oversight and on administrative traditions that accept the need to adapt methods to the systems under review.

The focus is intentionally concrete. Effective supervision depends on traceable data governance, inspection routines guided by operational risk, evidentiary standards for logs and metrics that can withstand scrutiny and testing environments in which failures can be

reproduced safely. These elements matter only if supervisory teams can question engineers directly and understand the answers well enough to act on them.

Taken together, the argument points to institutional capacities that strengthen oversight without multiplying formal requirements. Reliability, in this sense, is not a promise but a habit of acknowledging error and responding to it with discipline. The paper outlines how such habits can be developed within legal institutions and suggests how insights from Site Reliability Engineering may assist that process.

KEYWORDS

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

EXECUTIVE SUMMARY

Background: The supervision of digital infrastructures has entered a phase in which traditional legal methods struggle to capture the operational realities of modern systems. Automated pipelines, continuous deployments and data-driven adaptations mean that technical environments evolve while they run, often in ways that are difficult to reconstruct after the fact. Learning models compound this challenge by shifting internal decision paths in response to new inputs, rendering occasional inspections insufficient. Regulators who cannot follow at least part of this movement risk overlooking the precise moments at which routine disturbances escalate into genuine harm. Against this backdrop, a growing body of scholarship and regulatory practice has begun to treat operational awareness as an essential element of public responsibility.

Gap: Despite advances in algorithmic audits, impact assessments and risk-based supervision, most legal institutions continue to rely on policy declarations, post-hoc

reviews and assurances issued long after the relevant decisions have been executed. The capacity to obtain technical evidence that can be repeated, tested and defended in adversarial proceedings remains underdeveloped. Tracing data from origin to outcome, examining automated systems through risk-oriented audits and applying forensic standards to logs and metrics is far from routine in most supervisory agencies. This evidentiary weakness undermines both the credibility of oversight and the ability to distinguish ordinary fragility from genuine negligence.

Purpose: This paper proposes a capability model that aims to give legal practitioners a more grounded way of engaging with system behaviour. The intention is not to replace engineers but to equip supervisory teams with enough understanding to interpret what they observe and to translate technical artefacts into legally meaningful assessments. Drawing on the culture of reliability developed within Site Reliability Engineering, the analysis explores how concepts such as error budgets, service-level indicators and blameless post-incident reviews can inform legal doctrines of foresight, diligence and responsibility in automated environments.

Methodology: The analysis draws on regulatory experiences in Europe, where algorithmic audits and AI impact assessments are becoming embedded in supervisory practice, on Singaporean approaches that emphasise proportionality and risk-based oversight, and on Latin American administrative traditions that have adapted inspection methods to fast-moving technologies. It examines primary legal texts, regulatory guidance and scholarly commentary to identify the emerging contours of a law of technological risk. The paper further evaluates the practical tools that can support supervisory capacity, including inspection procedures grounded in operational risk, evidentiary standards for logs and metrics, controlled testing environments and adversarial exercises designed to expose weaknesses in system resilience.

Results: The study identifies several areas of supervisory capacity that require attention. These include a working fluency in code and system behaviour, defensible practices for data governance and lineage, auditing approaches shaped by risk rather than by formal compliance, and the ability to connect automated decisions with their consequences for ordinary users. None of this is viable without structured collaboration between legal and technical teams, particularly when engineers can explain system behaviour in operational rather than abstract terms. The paper also observes that SRE practices provide a useful framework for distinguishing failure from negligence. Error budgets translate abstract

duties of foresight into specific decisions about when to deploy and when to stabilise. Post-incident reviews, when documented with care, create records of cause, evidence and remedy that can withstand regulatory scrutiny. The absence of such documentation, by contrast, signals institutional neglect rather than mere misfortune.

Conclusion: Effective oversight of automated systems depends less on new declarations of principle and more on institutions capable of learning continuously. Regulators require training that moves beyond doctrinal comfort, procedures that hold up in litigation and a culture in which transparency is treated as part of the responsibility that comes with managing complex digital systems. Reliability, understood in this sense, is not a promise but a habit of acknowledging error and responding to it with discipline. A legal framework capable of distinguishing a documented, reviewed and corrected failure from a concealed or repeated one does not abandon sanction. It directs sanction toward institutions that refuse to learn. The convergence of legal norms and engineering practices offers the most promising path toward oversight that remains attentive to evidence, open to correction and clear about its purpose.

TABLE OF CONTENTS

Abstract
Keywords
Executive Summary
A. Introduction
B. The SRE Paradigm and the Culture of Reliability
C. Law of Technological Risk and Responsibility in Automated Environments
D. Redefining “Failure” and “Negligence” through the SRE Lens
E. Regulatory Implications and Challenges for Law
F. Conclusions
References

A. INTRODUCTION

Discussions about technological reliability have developed to a point where older assumptions about risk in automated, high-stakes environments no longer make sense. Systems built on automation, orchestration and continuous delivery treat error as part of their ordinary operation. A failure is rarely a dramatic exception. It is more often a predictable disturbance that needs to be measured, contained and used to improve the service that produced it. Legal analysis that still focuses on isolated faults struggles to capture how risk actually emerges in these architectures.

This tension has forced a closer exchange between engineers and legal practitioners. Across Latin America, concerns about algorithmic harm have encouraged supervisory bodies to adopt more proactive safeguards. In the United States, the NIST AI Risk Management Framework has begun to outline what measurable expectations for automated systems might look like, even if its practical influence remains uneven. What these developments share is the growing awareness that duties of foresight, traceability and timely response cannot be satisfied through document review alone. Supervision must reach the operational layer, where a system's behaviour is revealed rather than described (de Teffé and Medon, 2020).

Researchers have started to describe an emerging law of technological risk. It arises from the practical reality that agency in modern systems is distributed across people, code and infrastructure. Causation becomes less a straight line and more an attempt to reconstruct how design choices, operational routines and control mechanisms interacted over time. Developments in data protection and civil liability, particularly in Latin America, are already pushing legal doctrine in that direction. Governance duties, ex ante mitigation and coherent links between information, security and redress are becoming central organising principles. Scholarship in personal data protection has emphasised that prevention and responsibility depend on objective organisational duties and user-centred safeguards, ideas that sit comfortably beside technical practices such as observability and post-incident learning (Bioni and Dias, 2020).

The platform ecosystem intensifies these challenges. Platforms curate content, automate ranking and deliver essential services at scales that make classical oversight tools feel insufficient. Work on intermediary liability in the region has argued for standards that track actual functions, exposure to risk and real capacities for control. Notice regimes,

traceability and proportionate responses have become central themes. This body of doctrine helps shift the notion of reliability away from a technical aspiration and towards an institutional duty. It also reshapes how negligence should be understood when failures stem from structural weaknesses rather than from an individual's error (Palazzi, 2012).

The purpose of this section is to show how a culture of operational reliability can reshape the legal meaning of failure and negligence and how it might support a verifiable standard of reasonable technical care. Properly understood, reliability is an organisational position. It depends on the ability to anticipate incidents, absorb them without multiplying harm and learn from them through documented processes that can be examined with some rigour. Latin American administrative and civil law traditions already tie prevention and user protection to institutional responsibility. This provides a useful foundation for thinking about accountability in automated environments that accepts the inevitability of error without weakening the duty of care. The task is to connect legal prevention with technical risk management in a way that treats error as evidence rather than as an embarrassment to be concealed (de Teffé and Bodin de Moraes, 2017).

Courts and regulators will eventually have to confront a more uncomfortable point. Highly automated systems undermine the familiar boundaries on which both civil liability and administrative oversight were built. A model of negligence that imagines a single actor making a single mistake does not hold up when architectures are distributed, deployments are continuous and decision pathways are opaque. A law of technological risk will need to recalibrate its understanding of fault and diligence. Decisions about monitoring, documentation and recovery often play a larger causal role than any individual technical slip. Administrative bodies already have tools that could be adapted to support this form of structured responsibility, and civil liability can reinforce it by treating the absence of sound governance as a failure of care. Without such an operational lens, responsibility will continue to be assigned at the margins while the central sources of risk remain largely untouched.

B. THE SRE PARADIGM AND THE CULTURE OF RELIABILITY

Site Reliability Engineering developed from attempts to make complex technical systems manageable, but its lasting influence comes less from the tools it introduced and more

from the way it reshaped responsibility. When a team decides to track indicators that reflect real user experience, define service thresholds in clear terms and accept that a certain margin of failure is unavoidable, it creates a shared vocabulary that spans development, operations and management. Once that vocabulary exists, conversations about failure lose their dramatic tone. They become practical discussions about what can be changed without undermining the parts of the system that genuinely matter. Reliability ceases to be an optimistic assertion. It becomes something that has to be demonstrated.

The error budget illustrates this shift clearly. It is often described as permission for risk-taking, though in practice it operates as a constraint. Rising consumption slows deployments. Crossing the threshold stops them altogether unless there is a convincing reason to continue. Everything depends on the honesty of the metrics. If indicators are flattering rather than descriptive, risk accumulates quietly and emerges without warning. Scholars in Latin America have emphasised this problem for years. A system that chases numbers for their own sake is no safer than one that keeps no metrics at all. It simply becomes harder to audit and more difficult to hold accountable once something goes wrong (Melo, 2022; de Teffé and Medon, 2020).

Post-incident reviews conducted without seeking blame are often presented as matters of culture, but their real significance is institutional. When carried out with care, they form a record of how the system behaved, which assumptions failed and why certain remedial actions were selected. A thorough review is evidence of diligence even when the incident itself caused disruption. It shifts responsibility away from individual heroics and places it in documented practices of design, monitoring and correction. This aligns with regional legal doctrines that link responsibility to duties of prevention, transparency and continuous response rather than to the absence of reported failures (Doneda, Mendes and de Souza, 2020; Bioni and Dias, 2020).

For SRE to acquire real normative weight, a minimum evidentiary baseline must be available at any time. A service should be able to present the indicators that guide its decisions, the way these indicators reflect user outcomes, the thresholds that define acceptable behaviour and the points at which human intervention becomes necessary. It should also know how much of its error budget has been used and what recent incident reviews have concluded. These materials distinguish organisational structure from empty rhetoric. Their absence signals that SRE has not moved beyond vocabulary. This is especially visible in Latin American contexts, where data governance and user protection

regimes increasingly rely on objective organisational duties. The transparency expected in SRE mirrors legal expectations of traceability and helps give substance to a standard of reasonable care that is demonstrated through procedure rather than declared through intent (Bioni and Dias, 2020).

A recurring difficulty, however, is that some organisations adopt SRE language without altering the internal conditions that obstruct honest prioritisation. Dashboards multiply, yet the necessary conversations about what matters most do not take place. Reliability becomes a performance rather than a practice. It only becomes real when metrics have consequences. If the error budget is exhausted, new features do not ship. If recovery mechanisms reveal fragility, redesigns are delayed even when they are strategically attractive. These choices are costly, but they are the moments in which reliability becomes tangible. They are also the moments in which the law can recognise a form of technical diligence that has practical value rather than decorative appeal. Work on observability and operational risk across the region delivers a blunt message. Transparency without the capacity to act achieves little, and the capacity to act without any attempt to learn results in repeated failures.

Perhaps the most significant contribution SRE makes to legal analysis is the way it reframes negligence. The question shifts away from determining who pressed the wrong key and towards examining whether the system was designed to fail safely. Evidence is required that failure was anticipated, kept within manageable bounds and made recoverable. Under this view, negligence lies not in the existence of error but in the absence of structures that detect problems early, interpret them with evidence and correct them in a stable manner. This perspective brings technical practice closer to Latin American approaches that understand responsibility as a continuous task of governance, where prevention and remediation belong to the same cycle and diligence is assessed through documents, traces and operational processes rather than through assurances of quality (de Teffé and Medon, 2020).

C. LAW OF TECHNOLOGICAL RISK AND RESPONSIBILITY IN AUTOMATED ENVIRONMENTS

Legal systems have struggled for years to keep pace with technologies that learn, adapt and make decisions without waiting for anyone’s approval. Once algorithms begin

producing outcomes that even their own developers cannot fully anticipate, the older framework built around authorship, causation and blame starts to lose explanatory force. Law continues to search for a clear actor behind each decision, yet automated systems distribute agency across models, code, data pipelines and the infrastructure that supports them. The challenge is not subtle. What is needed is less the creation of a new doctrinal category and more a practical way of treating technological risk as something to be managed rather than eliminated. Canada's PIPEDA already asks organisations to shield individuals from the effects of automated decisions, and the GDPR in Europe expects some form of accountability for algorithmic processes. These instruments differ in method but respond to similar pressures (de Teffé and Medon, 2020).

In these environments, risk becomes part of routine operation instead of a rare anomaly. The relevant question therefore shifts. It is no longer whether systems will fail, because they will. It is how responsibility is shared when they do, who recognised the problem early and who bears the cost when the operational chain breaks. Engineering disciplines recognised this pattern earlier and built mechanisms to cope with error without systemic collapse. Legal analysis is catching up more slowly. Diligence can no longer be assessed by asking how many failures were avoided. It must be judged by whether institutions took reasonable steps to anticipate foreseeable harm and by how quickly they reacted when behaviour deviated from what was expected. This is a move toward an ex ante understanding of responsibility, where the emphasis falls on timely and reasonable management of risk rather than on the absence of incidents (de Teffé and Medon, 2020).

Another part of this shift is the gradual move away from individual fault and toward institutional responsibility. Automated systems are collective by design. Developers, operators, data providers, cloud platforms and the models themselves each contribute to the final outcome. Searching for a single culprit rarely produces clarity, and in many cases makes little legal sense. Attribution must instead turn to governance. Policies that define control, records of relevant decisions, traceable data flows and mechanisms for correction tend to offer a more reliable picture of technical care than any attempt to identify the individual who happened to interact with the system last. This perspective mirrors the culture of reliability in SRE, where responsibility is recognised in organisational routines rather than in the absence of isolated errors. For law, the lesson is not to replicate engineering tools but to accept that error forms part of the ordinary behaviour of complex systems and must be managed accordingly (Doneda, Mendes and de Souza, 2020).

Latin American scholars have pushed this line of reasoning further. They have shown how automation can magnify existing inequalities, leaving vulnerable groups at the mercy of opaque systems they cannot meaningfully challenge. Any credible account of technological risk must therefore consider its distributive effects. The point travels beyond the region. Canadian data protection law acknowledges it in the safeguards it imposes on automated decisions, and the GDPR's emphasis on transparency and accountability responds to the same concern. Harm tends to fall where protections are weakest. A law of technological risk that deserves the name must therefore balance efficiency with fairness, making sure the burdens created by automation do not settle on those with the least capacity to contest them (Melo, 2022; Bioni and Dias, 2020).

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

Engineers tend to speak about failure with a matter-of-fact clarity that legal analysis has long struggled to match. Within Site Reliability Engineering, failure is not treated as a dramatic rupture in an otherwise stable system. It is one of the predictable costs of operating large services that react to fluctuating demand, imperfect configurations and sudden changes in user behaviour. A spike in traffic can expose a flawed assumption in a scaling rule. A deployment script that has worked for months can fail at the one moment it matters. None of this surprises an SRE team. The relevant question is whether the organisation has designed its processes so these slips are detected early and their impact contained.

This logic translates directly to law. A failure is not automatically a legal problem. It becomes one when the organisation lacks a structured method for identifying the issue, analysing its causes and preventing recurrence. The global outage affecting Facebook, WhatsApp and Instagram on 4 October 2021 illustrates the point. A faulty configuration change disconnected Meta's backbone routers, propagating a failure that took its services offline for more than six hours. The firm later published a detailed post-mortem explaining the sequencing of events, the safeguards that failed and the remedial measures taken. From a legal perspective, that record is evidence of diligence: an institution acknowledging error, producing a traceable explanation and showing how it incorporated lessons for the future (Meta Engineering, 2021). By contrast, repeated failures without any documented attempt to learn from them signal something closer to institutional neglect.

A similar contrast was visible in the massive disruption suffered by Mercado Pago on 23 November 2022. Users across Latin America were unable to complete payments or transfers for several hours. The company confirmed service degradation but provided only a brief public statement and released no technical report that might shed light on root causes, safeguards or follow-up measures. The absence of documentation does not necessarily imply wrongdoing, but it limits the ability of regulators to understand the event and assess whether the response met a reasonable standard of care (Infobae, 2022). Vodafone España's nationwide outage on 4 February 2020 raised comparable concerns. Although the company acknowledged the incident and restored service gradually, public reporting revealed limited detail about why the system failed or how it planned to prevent similar events (Muñoz, 2020). The evidentiary gap becomes relevant when responsibility depends not on the occurrence of failure but on how the organisation responded.

The error budget sharpens this distinction. It sets an explicit tolerance for degradation and requires teams to slow or halt deployments when instability grows. Engineers often treat it as a limit on risk rather than a licence to take it. In legal terms, it translates abstract duties of foresight into specific decisions about when to deploy, when to roll back and when to stabilise. If a team delays an update because the error budget is nearly consumed, it is following a documented assessment of risk. The focus therefore shifts from isolated mistakes to the quality of the organisation's monitoring and decision-making structures, which aligns with regulatory approaches that prioritise prevention over punishment (Calo, 2021).

Seen from this perspective, negligence has little to do with the actions of one inattentive engineer. It reflects the failure of an organisation to build the routines needed to detect problems, track them and resolve them. A service that loses orders because no one checks error logs is not suffering from bad fortune. It is suffering from a lack of governance. The first mistake may be understandable. The refusal to learn from it is not. Scholars have stressed that accountability must be viewed as a structural rather than individual question, and automated systems make that shift unavoidable (Smuha, 2020).

Blameless post-incident reviews reinforce this approach. They are not exercises in assigning blame. They are structured efforts to reconstruct how the system behaved, how the failure surfaced and how recovery unfolded. When documented with care, they perform a function similar to a legal record. They establish a narrative of cause, evidence and remedy that can be examined by regulators. When no such record exists, it becomes easier to infer

negligence. The absence of documentation rarely means nothing happened. It often means that the institution did not want to look closely.

The idea of controlled failure also challenges earlier assumptions in legal doctrine. Not every deviation signifies fault. Some failures are expected and even planned. Systems absorb them without harm because safeguards exist. A brief interruption during maintenance is not comparable to an untested deployment that disables a banking platform. The distinction turns on preparation and response, not on the simple fact that something failed. Traditional doctrine, which tends to equate malfunction with blame, cannot survive contact with distributed architectures.

Reasonable technical care therefore demands a different understanding. It is not demonstrated by the absence of incidents but by the ability to maintain documentation, review assumptions, strengthen safeguards and incorporate lessons into routine practice. Reliability becomes a culture rather than a promise. Engineering provides the artefacts that make this visible. Law provides the expectation that these artefacts must reflect consistent, meaningful practice.

In this sense, SRE offers more than useful vocabulary. It provides a framework for distinguishing failure from negligence in environments where error is inevitable. Diligence lies in the response: whether the organisation understood what happened, recorded it and acted on it. Once law accepts this, it gains a clearer basis for assessing responsibility without ignoring the complexity of modern systems. The alternative is either fatalism or rigid sanction. A more realistic path lies between the two and rewards institutions that learn while exposing those that do not.

E. REGULATORY IMPLICATIONS AND CHALLENGES FOR LAW

Regulation has often assumed that technical systems become manageable once the right rules are written, as if control could be imposed from outside. Automated technologies make that assumption difficult to sustain. Engineers have long understood that complex systems fail in ways that are neither linear nor fully predictable. The Facebook–WhatsApp–Instagram global outage of 4 October 2021 made this plain on a public scale. A faulty configuration change propagated across Meta’s backbone network and removed the Border Gateway Protocol routes that allowed the company’s systems to be reachable on the internet. For nearly six

hours, global communication and commerce were disrupted despite the absence of a malicious attack. The incident showed how quickly an internal misconfiguration can cascade outward beyond the reach of conventional oversight (Frier, 2021). Legislating against every possible error achieves little. What matters is whether deviations are detected early, contained effectively and used to guide learning rather than denial. Aviation accepted this logic long ago by designing layered safeguards that begin from the expectation of error. Modern software systems, which propagate faults within seconds, make that lesson unavoidable (Smuha, 2020).

A regulatory approach grounded in reliability therefore pays less attention to how often an organisation stumbles and more to whether it understands what the stumble meant. The large outage that affected Vodafone España on 4 February 2020, which left thousands of users without service, illustrates the point. The company identified routing failures in its infrastructure and adjusted traffic management practices accordingly, producing a form of operational learning that no static compliance checklist could have generated (Muñoz, 2020). The shift here is subtle but important. Law has to move from inspecting outcomes to examining processes. Site Reliability Engineering's emphasis on routine error management shows how mistakes can become sources of insight rather than triggers for blame (Hood, Rothstein and Baldwin, 2001).

Regulators in different parts of the world are converging on this idea, even if their policy instruments differ. The European Union has adopted DORA for financial services and continues to refine the proposed AI Act. In the United Kingdom, the Information Commissioner's Office used the 2018 British Airways data breach to demonstrate that accountability requires evidence of monitoring, documentation and response. Although the initial fine proposed by the regulator was reduced, the case showed how supervisory bodies treat failures in system configuration, logging and security alerts as indicators of broader governance weaknesses rather than isolated mistakes (Information Commissioner's Office, 2020). In the United States, the release of NIST's AI RMF 1.0 in early 2023 reflects an attempt to provide regulators and industry with a shared vocabulary for assessing AI risk. Singapore's 2020 governance framework remains influential in Asia, while Japan and South Korea experiment with their own models of oversight. Across Latin America, financial supervisors are beginning to explore digital resilience models that prioritise process over static inspection. These trends all point in the same direction: governance that follows systems as they evolve.

The central challenge is cultural as much as legal. Many legal systems still equate error with wrongdoing. Blameless reviews can therefore seem unfamiliar, yet they provide insights that formal investigations rarely achieve. An online marketplace that identifies an overloaded server as the cause of an outage and updates its load-testing practices has shown diligence in a way that classical doctrine might overlook. By contrast, punitive environments tend to push organisations toward concealment. A supervisory model that rewards clear and timely incident reporting encourages improvement rather than evasion (Smuha, 2020).

A mature law of technological risk would create conditions in which organisations can disclose problems without fearing disproportionate penalties. This is not an argument for leniency. It is an argument for learning. A cloud service that publishes a detailed account of an outage offers greater protection to its users than one that pays a fine while revealing little. Public scrutiny of incident logs allows a more grounded assessment of whether institutions understand their systems and whether they have addressed the underlying causes of failure (Hood, Rothstein and Baldwin, 2001).

For this to work, regulators themselves need to evolve. Oversight cannot rely solely on doctrine. It requires a working familiarity with code, system architectures, operational behaviour and the evidentiary value of logs and metrics. Paper-based inspections are of limited use when systems change multiple times per hour. Regulators need to work alongside engineers to translate technical artefacts into supervisory judgment. Europe has already begun training regulators in algorithmic audits and AI impact assessment. Singapore's risk-focused audits push supervisors to understand system behaviour directly. Latin America, although slower to formalise these practices, benefits from administrative traditions that adapt pragmatically to evolving technologies (Doneda, Mendes and de Souza, 2020).

Ethics underpins this entire discussion. Treating error as a normal feature of automation must not justify careless design or unsafe practices. Controlled failure only makes sense when users are protected and when tolerance remains within socially acceptable boundaries. Regulation should not become paralysed by an unattainable vision of perfection, but nor should it slide into permissiveness. The task is to strike a balance that maintains trust. In that balance, law can reposition itself not as an obstacle to innovation but as a guardian of the public confidence that innovation requires. A culture of reliability built around shared responsibility, institutional learning and honest repair sits exactly at the intersection between technical logic and the demands of justice.

F. CONCLUSIONS

The relationship between technological reliability and legal responsibility is no longer an abstract discussion. It unfolds daily in systems that fail while real users watch and in institutions that must decide whether those failures reflect ordinary fragility or a deeper absence of care. Engineers have spent years refining methods to keep services stable under pressure and to extract lessons from the moments when stability breaks. Law is beginning to recognise that its own legitimacy depends on something similar. General principles help, but they do not replace the need for verifiable evidence about how systems behave. Site Reliability Engineering offers one practical route into that evidentiary discipline by insisting that infrastructures must be observable, measurable and open to scrutiny (NIST, 2023; European Commission, 2018).

Recent regulatory developments point in the same direction. The publication of NIST's AI RMF 1.0 signals a willingness to evaluate automated decision-making in concrete terms. Canada's PIPEDA ties accountability to meaningful explanations. Europe's GDPR pressures organisations to confront the opacity of their systems. Singapore's 2020 framework adds a model of supervision organised around risk. None of these instruments promises the elimination of failure. Their shared message is both simpler and more demanding: systems must document their behaviour, acknowledge how they fail and show what they learned.

Once responsibility is analysed through the lens of reliability, the legal timeline begins to shift. The assumption that harm comes from a single discrete event becomes harder to maintain in environments where systems generate continuous micro-decisions and where harm often emerges cumulatively. Continuous observation becomes central to supervision. Diligence stops being an impressionistic standard and becomes something that can be demonstrated. Error budgets, service indicators and post-incident reviews move from engineering artefacts to legal evidence: records of what an organisation understood, when it understood it and how it responded. Prudence becomes something that can be shown rather than stated.

Latin American scholarship adds an ethical dimension that is sometimes underestimated elsewhere. In societies marked by inequality, the consequences of technical failure fall unevenly. Reliability becomes not only a question of design but of fairness. This intuition travels well. Whether in European guidance, NIST's recommendations or OECD

principles, a common insight is emerging: public trust grows through transparent practices rather than through increasingly dense rulebooks (NIST, 2023; OECD, 2019; European Commission, 2020). For regulation to remain legitimate, it must rely less on formal control and more on the quality of the procedures that sustain it.

A law of technological risk should resist the temptation to force systems into predictable shapes. It has to work with uncertainty and design frameworks that absorb shocks without collapsing. Engineering shows that resilience is built through design, monitoring and learning. Law can reinforce this by requiring documentation, traceability and audits that reveal how institutions respond to error. The aim is not heavier control but stronger institutional memory. An organisation that keeps and analyses its incident history is not just avoiding negligence. It is building a form of trust that legal systems can recognise and protect.

The most significant change ahead is likely to be cultural. Accepting that systems fail does not justify irresponsibility. It reflects a practical understanding of human and technical limits. Responsibility shifts from preventing every failure to responding to failures with clarity and discipline. A documented, reviewed and corrected failure is evidence of maturity. A concealed or repeated failure is something closer to negligence. A legal framework capable of distinguishing between the two does not abandon sanction. It directs it toward institutions that refuse to learn.

If contemporary risk theory teaches anything, it is that SRE offers a useful guide for the legal transition now underway. It encourages regulators to focus on learning rather than control for its own sake. It suggests that the aim is not to eliminate harm but to convert experience into knowledge and to maintain supervision that adapts as systems evolve. Law does not need to outrun technology. It needs a way of engaging with it that remains attentive to evidence, open to correction and clear about the purpose of oversight (Hood, Rothstein and Baldwin, 2001). Only then will legal institutions be prepared to govern the systems upon which society increasingly depends.

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. https://doi.org/10.1146/annurev-lawsocsci-101620-013809

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* (AR/JUR/46837/2018). La Ley Online.

de Teffé, C. S., & Bodin de Moraes, M. C. (2017). Redes sociais virtuais: Privacidade e responsabilidade civil. *Pensar, 22*(1), 108–146. https://doi.org/10.5020/2317-2150.2017.6084

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. https://doi.org/10.21783/rei.v6i1.437

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. https://doi.org/10.5020/2317-2150.2020.9808

European Commission. (2018). *Regulation (EU) 2016/679 (GDPR)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Commission. (2020). *Proposal for a regulation on digital operational resilience for the financial sector (DORA)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595

European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Commission. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554

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)*. https://laws-lois.justice.gc.ca/

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

Infobae. (2022, November 23). *Se cayeron Mercado Libre y Mercado Pago: los usuarios reportaron problemas para operar con la plataforma*. https://www.infobae.com/economia/2022/11/23/se-cayeron-mercado-libre-y-mercado-pago-los-usuarios-reportaron-problemas-para-operar-con-la-plataforma/

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. https://doi.org/10.1007/s43681-021-00104-8

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)*. https://doi.org/10.6028/NIST.AI.100-1

Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on Artificial Intelligence*. OECD Publishing. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

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

Siddiqui, F. (2021, October 5). *Facebook, Instagram and WhatsApp suffer global outage*. The Washington Post. https://www.washingtonpost.com/technology/2021/10/04/facebook-down-instagram-whatsapp/

Vodafone outage — Spain. (2020, February 19). In R. Muñoz, *Una avería deja sin servicio a miles de clientes de Vodafone*. *El País*. https://elpais.com/economia/2020/02/19/actualidad/1582102382_369209.html