The Evolution of Cyber Tort Liability: Conceptual Challenges in Algorithm-Induced Harm

1. Daniel Tremblay: Department of Political Science, University of Toronto, Toronto, Canada
2. Jennifer Lee*: Department of Political Science, Stanford University, Stanford, USA
3. Amelia Lawson: Department of Law, University of Sydney, Sydney, Australia
*****Correspondence: e-mail: jennifer.lee@stanford.edu

Abstract

The rapid advancement of algorithmic and autonomous decision-making systems has fundamentally reshaped the nature, sources, and pathways of harm in the digital age, challenging the foundational assumptions of traditional tort law. As machine learning, predictive analytics, and neural networks increasingly influence medical, commercial, administrative, and social environments, legal systems struggle to reconcile long-standing doctrines with emerging forms of injury that arise from opaque, adaptive, and probabilistic computational processes. This narrative review adopts a descriptive–analytic approach to examine the historical evolution of cyber tort liability, beginning with early internet harms such as defamation, intrusion, software negligence, and cybersecurity breaches, and moving through transitional phases marked by platform liability debates and the growing influence of algorithmic content curation. The review then analyzes the conceptual and doctrinal tensions exposed by algorithm-induced harms, including challenges of causation, foreseeability, duty of care, standard of reasonableness, attribution, vicarious liability, and the classification of algorithms as products, services, or sui generis entities. It further surveys emerging regulatory responses across jurisdictions, including the European Union's risk-based AI governance approach, the fragmented U.S. reliance on traditional tort principles and platform immunity, the nuanced common-law adaptations in the UK, Canada, and Australia, and Asia's increasingly administrative models of algorithmic oversight. International soft-law instruments are also examined for their role in harmonizing global approaches. The review concludes that algorithmic systems generate structural contradictions within tort doctrine, revealing the need for conceptual reframing and new liability models that can accommodate distributed agency, systemic harms, and technological opacity. These insights offer a foundation for future legal scholarship and policy development aimed at ensuring accountability in an era defined by autonomous digital systems.

Keywords: Cyber tort liability; algorithm-induced harm; artificial intelligence; legal responsibility; causation; duty of care; autonomous systems; algorithmic governance; digital regulation; emerging technologies

Received: date: 11 May 2023
Revised: date: 10 June 2023
Accepted: date: 25 June 2023
Published: date: 01 July 2023

Citation: Tremblay, D., Lee, J., & Lawson, A. (2023). The Evolution of Cyber Tort Liability: Conceptual Challenges in Algorithm-Induced Harm. *Legal Studies in Digital Age*, 2(3), 49-63.

1. Introduction

The emergence of algorithmic systems, autonomous decision-making tools, and data-driven digital platforms has fundamentally altered the landscape of harm, responsibility, and regulation in contemporary society. What was once a domain defined primarily by human actions has gradually shifted into a technologically mediated environment in which algorithms perform tasks, make predictions, and influence decisions that can profoundly affect individual rights and social structures.

Scholars examining the implications of artificial intelligence on professional and public life have observed how pervasive AI adoption, particularly in fields such as healthcare, significantly transforms decision pathways and amplifies risks associated with automated processes, as seen in discussions of augmented medical decision-making by radiologists in Saudi Arabia (Alyami et al., 2021). These transformations underscore the ways advanced systems increasingly operate as quasi-autonomous actors whose decisions may generate unique forms of harm that traditional tort frameworks struggle to address. As Chagal-Feferkorn notes, even the determination of whether an algorithm acted "reasonably" challenges evaluative standards that were originally constructed around human behavior rather than machine-driven prediction (Chagal-Feferkorn, 2021). The algorithmic age, therefore, calls into question foundational assumptions that underlie tort law, particularly those relating to foreseeability, causation, and the nature of agency.

The evolving complexity of these systems reveals that digital environments are not simply extensions of physical contexts but are instead novel domains of interaction defined by automated data processing, predictive analytics, and autonomous recommendations. Scholars have highlighted that AI systems exhibit forms of independence and opacity that distinguish them from earlier computational technologies, with legal commentators emphasizing the growing difficulty in attributing responsibility for outcomes produced through machine-learning architectures (Tretyakova, 2021). The opacity inherent in complex neural models, often referred to as the "black-box problem," has significant effects on tort doctrine, as victims may struggle to demonstrate how algorithmic processes contributed to harm. This difficulty is compounded by the fact that autonomous systems often evolve over time through their exposure to new data, rendering their actions not fully predictable even to their developers. As a result, harm induced by algorithms frequently resists the categories developed for conventional torts, which assume a clear causal chain between a human actor and an actionable injury. The legal system's struggle to adapt to algorithmic harms is evident in multiple jurisdictions, where scholars have identified the increasing irrelevance of conventional liability models when confronting autonomous agents (Huberman, 2020).

Cyber torts represent a crucial conceptual bridge between traditional tort law and the new realities of algorithmically mediated harm. In general terms, cyber torts refer to civil wrongs committed through or arising from digital systems, such as online defamation, breaches of data protection, harmful algorithmic recommendations, automated discrimination, and unauthorized surveillance. Although the term encompasses familiar tortious concepts—such as negligence, misrepresentation, and trespass—its application to digital contexts alters their structure and interpretation. For example, micro-targeted misinformation disseminated by automated content systems presents new forms of reputational harm distinct from traditional defamation, as highlighted in analyses of AI-driven communication platforms and their ethical complexities (Zelinski, 2023). Similarly, medical AI systems that generate diagnostic recommendations can cause clinical harm without any direct human intervention, a possibility that has led legal scholars to question whether existing tort principles can adequately assess the role of algorithmic error (Gayvoronskaya & Galchun, 2021). The central issue is that cyber torts are not merely digital versions of traditional torts; they are structurally different because the digital environment fundamentally reshapes the relationship between action, intention, and injury.

Another distinguishing factor of cyber torts is the pivotal role of data. The quality, structure, and origin of data directly shape algorithmic outputs, meaning that harm may arise not from the apparent behavior of a system, but from subtle inaccuracies, embedded biases, or incomplete datasets. Studies on the integration of AI into healthcare demonstrate that data-driven processes introduce layers of uncertainty and risk, especially when large datasets contain hidden biases that become magnified through automated decision-making, as noted in assessments of how big data influences clinical systems (Moodley, 2023). This emphasis on data complicates traditional tort concepts, since responsibility in the data pipeline may be diffuse, involving developers, data collectors, platform managers, and algorithmic designers. Legal analyses of AI implementation in medical robotics echo this fragmentation of responsibility, pointing out that the collective nature of AI development disperses liability across multiple actors (O'Sullivan et al., 2019). Cyber tort liability, therefore, requires a more granular understanding of the distributed nature of digital harm.

The rise of algorithm-induced harms is especially evident in contexts where predictive algorithms shape decision-making outcomes with societal consequences. In discussions of liability allocation, Tretyakova observes that even when AI systems support healthcare providers, errors embedded in algorithms may shift responsibility away from human actors while simultaneously leaving gaps in legal accountability (Tretyakova, 2021). Comparable concerns emerge in cybersecurity contexts, where algorithmic systems autonomously respond to threats and may inadvertently escalate vulnerabilities or cause collateral harm, as explained in analyses of machine learning used to fortify healthcare cybersecurity (Mosaddeque et al., 2022). These examples demonstrate that algorithm-induced harms often flow from the intricate interplay between system design, data processing, and autonomous decisions, making it difficult to trace wrongdoing to a single responsible agent. Tort law, built on assumptions of individual agency, intention, and direct causality, is ill-equipped to navigate these intricate causal webs.

Another feature of algorithm-induced harm is the potential for systemic and large-scale effects. Algorithmic amplification, for instance, can escalate misinformation, propagate harmful stereotypes, or enhance discriminatory outcomes across vast populations. Scholars examining AI's social and structural consequences underline the dangers of algorithmic manipulation and the ways it can contribute to broader societal harms, including the reinforcement of inequities through automated reasoning (Dyson, 2022). The potential for collective harm distinguishes algorithmic risks from traditional torts, which tend to focus on discrete incidents rather than systemic distortions. This systemic dimension has prompted calls for new legal frameworks that can capture the cumulative effects of algorithmic processes, especially when harms emerge gradually or indirectly from the operation of long-running systems.

The problem of foreseeability remains central to understanding the conceptual challenges underlying cyber tort liability. Traditional tort law relies on the ability to assess whether a reasonable actor could foresee the harm that occurred. The use of deep learning systems complicates this assessment because developers may not fully understand how outputs are generated. Cestonaro's systematic review of medical diagnostic algorithms illustrates that the unpredictable nature of machine learning models frequently obstructs the application of classical foreseeability standards (Cestonaro et al., 2023). This unpredictability challenges courts to determine whether system developers, hospitals, or algorithmic vendors should be held liable for harm that even experts cannot foresee. The inability to reliably predict algorithmic outcomes erodes one of the most important pillars of tort doctrine and underscores why cyber tort liability requires an updated theoretical foundation.

The difficulty of identifying the relevant actor in algorithm-induced harm further complicates liability frameworks. Some scholars argue that algorithms themselves should be considered potential bearers of responsibility or at least be recognized as entities with limited legal personhood, reflecting the fact that they increasingly perform tasks once conducted by humans (McDonald, 2023). Others assert that responsibility must remain with the human agents who design, train, or deploy AI systems, as relying on machine personhood could absolve corporations of meaningful accountability (Gallese, 2022). The debate around whether AI can or should possess legal personality reveals deeper disagreements about the role of autonomy, agency, and moral responsibility within digital ecosystems. This debate is essential for understanding cyber tort liability, since the question of who—or what—constitutes the tortfeasor is no longer straightforward.

The healthcare domain, which has been a primary testing ground for AI deployment, provides significant insight into the liability challenges associated with algorithmic decision systems. Analysts exploring medical AI have emphasized that the integration of autonomous systems into clinical workflows blurs professional duties and complicates the assignment of responsibility when harm occurs (Ganapathy, 2021). Ethical evaluations of AI in clinical contexts further highlight that harm may arise not only from algorithmic error but also from improper deployment, inadequate supervision, or misuse of automated systems (Elendu et al., 2023). These inquiries reveal how cyber tort liability is deeply intertwined with professional standards, institutional practices, and evolving expectations of algorithmic reliability.

Because traditional standards of care rely on human competencies, applying them to algorithmic contexts is inherently problematic. Bashayreh's examination of legal standards in AI environments calls attention to the inadequacy of conventional duty-of-care concepts when systems act without direct human oversight (Bashayreh et al., 2023). Without a clear benchmark for algorithmic reasonableness, courts face difficulties determining whether developers or users failed to meet their legal obligations. The problem extends beyond negligence to product liability, where commentators highlight that AI systems often do not fit neatly into existing definitions of "product," making it difficult to apply strict liability principles (Bączyk-Rozwadowska, 2022). As cyber torts increasingly arise from intersections of software, data, and automated processes, legal scholars continue to question whether new classifications or hybrid models of liability are required.

The international dimension of algorithmic harm also plays a vital role in shaping cyber tort debates. AI systems often operate across borders, raising questions of jurisdiction, conflict of laws, and regulatory harmonization. Discussions on revising European liability models for smart robots illustrate the need for coherent transnational frameworks capable of addressing cross-jurisdictional harms produced by autonomous systems (Gallese, 2022). Meanwhile, analyses of legal approaches in Russia emphasize the varied conceptualizations of civil liability in AI development and deployment, reflecting differences in national legal traditions and policy priorities (Kharitonova et al., 2022). These global divergences demonstrate that cyber tort liability is emerging in a complex, fragmented regulatory environment that lacks consistent principles for addressing algorithm-induced harm.

As these challenges illustrate, the evolution of cyber tort liability involves both conceptual and practical transformations. Algorithmic harms are decentralized, probabilistic, data-dependent, and often opaque. They disrupt established legal doctrines by complicating the identification of causal relationships, blurring distinctions between product and service, and challenging notions of intent and foreseeability. Moreover, scholars emphasize that algorithmic systems frequently reshape institutional norms and expectations, creating new pressures for courts and legislatures to adapt legal doctrine to evolving technological realities (Sqalli et al., 2023). These complexities reveal why cyber tort liability demands a more holistic and interdisciplinary approach that integrates legal theory, technical understanding, ethical analysis, and regulatory innovation.

The purpose of this narrative review is to explore the conceptual evolution of cyber tort liability and to analyze the doctrinal challenges posed by algorithm-induced harms. The review seeks to describe how tort law has responded to new forms of digital harm, identify the gaps that hinder effective accountability, and examine emerging legal and regulatory solutions across jurisdictions. The guiding questions focus on how algorithmic systems reshape foundational tort concepts, how responsibility should be allocated within complex data-driven ecosystems, and what adaptations are required for tort law to remain effective in the algorithmic era.

2. Historical Evolution of Cyber Tort Liability: From Early Internet Harms to Algorithmic Decision Systems

The historical evolution of cyber tort liability began with harms arising from the early architecture of the internet, where the primary concerns revolved around conventional tort concepts applied to novel digital environments. Early cyber harms typically emerged from online defamation, intrusion into digital spaces, software-related negligence, and data breaches. These harms resembled traditional tortious behavior but manifested in settings shaped by new technologies. The expanding communicative capabilities of early internet platforms, such as blogs and anonymous forums, generated reputational injuries that courts struggled to evaluate under existing defamation standards, particularly when algorithmic indexing tools elevated the visibility and longevity of harmful statements. Ethical and legal discussions on the role of technology in reshaping professional practices demonstrate how digital tools increasingly mediated interpersonal interactions, such as in healthcare settings where automated systems influenced diagnostic communication (Alyami et al., 2021). These early developments foreshadowed broader difficulties in assigning liability in technologically mediated contexts, where the actors responsible for harm might include not only human users but also system designers and platform administrators. Concerns about defective software and negligent system maintenance further complicated traditional negligence frameworks, as digital failures often resulted from complex interactions between code, hardware, and user behavior. Legal theorists exploring responsibility in technologically enriched domains identified the need for doctrines capable of addressing indirect and distributed harms, which became evident in multi-layered AI-assisted environments (Gayvoronskaya & Galchun, 2021).

As digital technologies matured, a transitional phase emerged in which social media platforms, interactive websites, and global communication infrastructures redefined the scope of liability. The central issue during this period was the liability of intermediaries, particularly platforms hosting user-generated content. Courts and legislatures across multiple jurisdictions grappled with whether and to what extent online platforms should bear responsibility for harmful speech and conduct committed by users. Scholars analyzing the development of AI-enabled communication tools noted that automated moderation systems and algorithmic curation introduced additional layers of complexity, as these systems began shaping user interactions and amplifying certain types of content (Zelinski, 2023). This transition intensified the debate over the applicability of doctrines such as Section 230 in the United States, which shielded intermediaries from liability for content posted by third parties, and similar immunity provisions in other regions. Legal theorists examining the evolving responsibilities of digital intermediaries highlighted the tension between protecting platform innovation and ensuring accountability for harm facilitated or amplified by automated systems (Huberman, 2020). During this phase, user-generated content created a new environment in which harm could result not only from direct human action but also from the design choices of platforms that structured communication flows, as seen in discussions of cyber risks and automated data-processing tools (Mosaddeque et al., 2022). The interplay between human expression and algorithmic distribution demonstrated that intermediary liability could no longer be considered solely in relation to user behavior; instead, the technological architecture of platforms shaped the likelihood, scope, and scale of harm.

The evolution of intermediary liability coincided with technological innovations that led to the emergence of autonomous and semi-autonomous digital systems. The introduction of machine learning, neural networks, predictive algorithms, and recommendation engines signaled a paradigm shift in which computational processes increasingly produced decisions independently of direct human control. Analysts of AI in healthcare have described how diagnostic algorithms developed the capacity to operate as semi-autonomous agents capable of evaluating images and recommending treatment pathways, raising questions about whether responsibility should attach to the programmer, the healthcare provider, the institution, or the algorithm itself (Cestonaro et al., 2023). Scholars examining the legal and regulatory implications of using autonomous systems in high-risk fields similarly identified the problem of attributing liability in contexts where algorithms rely on complex data-processing strategies and adaptive learning mechanisms (O'Sullivan et al., 2019). This shift prompted the reconsideration of foundational tort principles such as intent, foreseeability, and causation. The introduction of self-modifying algorithms magnified these challenges because their decisions were not entirely predictable even to their creators. As legal theorists noted, algorithms that adjust their internal models over time through exposure to new data create dynamic conditions that strain conventional liability theory (Tretyakova, 2021). The increasing automation of decision systems, particularly in sectors such as healthcare, finance, transportation, and content moderation, exposed the inadequacy of tort doctrines designed for human actors operating under stable and predictable behavioral patterns.

As algorithmic systems expanded their influence across sectors, new categories of digital harm began to surface, requiring doctrinal innovation and scholarly reassessment. Informational harm emerged as a distinct category, reflecting injuries that arise not from physical or financial damages but from the manipulation or distortion of information through automated processes. In healthcare, for example, algorithmic misclassification or erroneous data interpretation can directly shape treatment decisions, illustrating how informational harm can lead to tangible injury, as described by researchers studying the integration of AI into clinical workflows (Ganapathy, 2021). Another category involved algorithmic discrimination, where biased training data or flawed model architectures produced unequal treatment across demographic groups. Scholars examining AI ethics have underscored the risks of embedded bias in diagnostic and decision-support systems, noting that inadequate algorithmic design can disproportionately affect vulnerable populations (Elendu et al., 2023). Automated misinformation diffusion constituted yet another expanding category of harm. Recommendation engines and predictive models used by digital platforms often amplify sensational or polarizing content because it increases engagement, inadvertently contributing to the spread of misinformation. Observers of AI-driven communication technologies have highlighted how these systems play a role in disseminating misleading or harmful narratives, with significant implications for public discourse (Dyson, 2022). These categories reveal that algorithmic harms often operate at a structural level, shaping information ecosystems, distorting user behavior, and producing consequences that extend beyond individual disputes into collective and systemic vulnerabilities.

Legal systems across jurisdictions responded unevenly to the changing landscape of digital harm, producing a complex patchwork of doctrinal innovations, regulatory experiments, and jurisprudential divergence. Some jurisdictions adapted existing tort principles to emerging harms by stretching negligence doctrines to include failures in system design, inadequate data governance, or insufficient algorithmic oversight. Legal scholars examining AI deployment in medical environments emphasized that courts increasingly consider whether institutions maintained adequate supervision of algorithm-driven systems and whether developers exercised reasonable care in training models and managing data inputs (Bashayreh et al., 2023). Other jurisdictions introduced new legal categories or regulatory requirements intended to fill gaps left by traditional tort frameworks. European commentators have analyzed reforms aimed at addressing liability for smart robots and autonomous systems, arguing for updated standards better aligned with algorithmic complexity (Gallese, 2022). In contrast, some countries focused on clarifying civil liability principles for AI and robotic systems, as seen in Russian academic discussions highlighting the challenges of aligning national doctrines with rapidly evolving technologies (Kharitonova et al., 2022). These varied responses reflected not only differences in legal traditions but also divergent political and economic priorities related to technology governance.

Over time, courts and legal scholars increasingly recognized that algorithmic decision systems created forms of causation that did not align with linear, human-driven models. The challenge of identifying causal chains in algorithmic environments is frequently acknowledged in studies examining how computational processes shape outcomes without producing human-readable reasoning (Chagal-Feferkorn, 2021). Traditional tort doctrines presuppose a clear link between action and injury, but algorithmic harms often arise from distributed processes involving data collection, model training, iterative improvement, and automated deployment. As these systems became more sophisticated, the inadequacy of standard doctrines became more apparent. Analysts exploring AI's impact on healthcare have described scenarios in which multiple contributors—including data suppliers, developers, medical practitioners, and autonomous models—all play roles in the production of harm, making singular liability assignments increasingly impractical (Moodley, 2023). This distributed causation has pushed legal theorists to reconsider whether tort law should move toward strict liability models, hybrid compensation schemes, or entirely new categories of algorithmic responsibility.

A significant influence on the evolution of cyber tort liability has been the growing recognition that algorithmic systems operate as socio-technical infrastructures rather than discrete tools. Scholars examining biomedical and technological research have noted that digital systems increasingly shape scientific inquiry and professional behavior, revealing how deeply embedded automated processes have become in modern institutional contexts (Brogan, 2021). The embedded nature of automated systems complicates liability analysis because harms may occur not from isolated algorithmic mistakes but from structural dependencies that organizations develop around automated decision-making. For example, as machine learning systems become central to diagnostic procedures or risk assessments, human decision-makers may defer to algorithmic recommendations, leading to heightened reliance on systems whose internal mechanisms remain opaque (Cestonaro et al., 2023). This reliance contributes to a shift in professional expectations, necessitating the development of policies and doctrines capable of managing both direct algorithmic failures and secondary harms arising from institutional dependence on automated tools.

The increasing reliance on algorithmic systems has also expanded the temporal and spatial dimensions of harm, challenging traditional jurisdictional frameworks. Automated recommendations, risk scores, and decision outputs circulate across borders instantaneously, raising questions about which jurisdiction's liability rules should apply. Discussions surrounding the global standards for AI in medical robotics underscore the need for harmonized legal frameworks capable of managing transnational digital interactions (O'Sullivan et al., 2019). Divergent national approaches to liability for AI systems demonstrate that the evolution of cyber tort doctrine is shaped by cultural, legal, and technological factors unique to each jurisdiction. Analysts exploring Russian legal approaches emphasize that conceptual differences in understanding AI agency and responsibility contribute to varied doctrines across legal systems (Kharitonova et al., 2022). In contrast, European reforms reflect a strong regulatory drive to integrate AI-specific liability principles into broader digital governance strategies (Gallese, 2022). This fragmentation presents ongoing challenges for victims seeking redress and for developers operating in global markets.

As the historical evolution of cyber tort liability demonstrates, the transition from early internet harms to algorithm-induced injuries is marked by increasing technological complexity, shifting legal expectations, and expanding categories of risk. Traditional tort principles proved adaptable during the early stages of digital transformation, when harms still originated primarily from human actors operating within digital spaces. However, as semi-autonomous and autonomous systems became more prevalent, these principles encountered conceptual limits. Scholars studying digital ethics, intermediary responsibility, and autonomous decision-making have consistently shown that algorithmic systems reshape the tort landscape in ways that challenge foundational assumptions about intentionality, foreseeability, causation, and agency (Sqalli et al., 2023). This historical trajectory illustrates how tort doctrine, once suited to relatively straightforward analyses of individual wrongdoing, must now confront increasingly complex causal networks that involve human actors, digital platforms, data ecosystems, and autonomous algorithms.

The evolution of cyber tort liability reveals the need for frameworks capable of addressing harms generated not only through human misuse of digital systems but also through the intrinsic characteristics of algorithmic processes. As algorithmic decision systems become more deeply entrenched across sectors, the doctrinal tools developed during earlier phases of digital transformation are no longer sufficient to ensure accountability. Understanding this evolution provides the foundation for analyzing the conceptual and doctrinal challenges explored in subsequent sections of this narrative review.

3. Conceptual and Doctrinal Challenges in Assigning Liability for Algorithm-Induced Harm

The conceptual and doctrinal challenges in assigning liability for algorithm-induced harm stem primarily from the difficulty of establishing causation within systems that function according to complex, opaque, and probabilistic mechanisms. Traditional tort doctrines assume that harmful conduct can be traced to discrete acts or omissions committed by identifiable human agents. Yet algorithmic systems, particularly those built upon deep learning and neural network architectures, produce outputs through computational processes that even their designers may not fully understand. Scholars studying diagnostic algorithms in medicine explain that the internal logic of machine learning systems can be resistant to interpretation, thereby creating evidentiary barriers for plaintiffs attempting to demonstrate causal relationships between system behavior and resulting injuries, a difficulty highlighted in systematic analyses of AI-driven diagnostic tools (Cestonaro et al., 2023). The opacity of algorithmic processes, often referred to as the "black box" problem, complicates foreseeability as well, since developers cannot always anticipate how models will behave after being exposed to new data. Legal theorists examining autonomous-machine-caused harms describe how unpredictability undermines classical tort presumptions about what a reasonable actor could foresee (Huberman, 2020). This intertwining of opacity and unpredictability makes it challenging for courts to apply traditional causation tests such as the "but-for" test or the substantial-factor test, because algorithmic systems may produce harmful outcomes without a clear or discoverable chain of reasoning.

The challenge of causation is heightened by the probabilistic nature of algorithmic outputs. Machine learning systems generate predictions or classifications based on statistical correlations rather than deterministic logic, meaning their outputs inherently carry uncertainty. Analysts studying how AI transforms healthcare emphasize that these probabilistic outputs, while often highly accurate, can introduce significant risk because they operate without human-level contextual understanding, thereby raising questions about whether harm arises from system design, flawed data, or unpredictable model behavior (Moodley, 2023). Evidentiary burdens in tort litigation rely on showing that harm was more likely than not caused by the defendant's actions, yet probabilistic models complicate such demonstrations because their operations rely on complex statistical processes. The black-box nature of these systems obstructs the ability of plaintiffs to access or interpret the underlying mechanisms needed to prove causation. Courts may struggle to differentiate between systems functioning as expected, systems functioning defectively, and systems producing reasonable but harmful outputs based on flawed or biased training data. Scholars observing AI's influence on professional reasoning also note that automated systems can guide human decision-makers in ways that create layered causal structures, further complicating evidentiary analysis (Brogan, 2021). As algorithmic systems become increasingly autonomous, traditional evidentiary frameworks risk becoming obsolete, thereby revealing a profound doctrinal limitation in tort law.

Duty of care represents another major area in which traditional tort principles encounter structural inadequacies in digital ecosystems. Determining what constitutes a reasonable duty of care for developers, data scientists, platform operators, and end users becomes difficult when technologies evolve rapidly and behave in unexpected ways. Studies exploring civil liability in AI and robotic systems emphasize that duty cannot be conceptualized solely in terms of individual agency because AI development involves inputs from numerous actors whose responsibilities overlap or conflict (Kharitonova et al., 2022). For example, a developer may design an algorithm according to best practices, yet the operator may deploy it in a context for which it was not originally intended. Research examining AI responsibility in healthcare highlights that medical institutions increasingly rely on AI support systems, thereby redistributing professional duties between clinicians and automated tools (Tretyakova, 2021). When these systems malfunction or produce flawed recommendations, determining whether developers failed to meet their duty of care or whether practitioners failed in oversight becomes a challenging evaluative question. Ethical investigations into AI deployment in healthcare settings further underscore the difficulty of assigning duties because AI systems often assume roles that blur the boundary between tool and decision-maker, thereby transforming expectations around human oversight (Elendu et al., 2023).

The standard of reasonableness in negligence law faces substantial theoretical strain when applied to systems capable of autonomous learning and adaptation. Reasonableness assumes that human actors behave according to stable norms of conduct, but algorithmic systems may evolve in unpredictable ways due to dynamic learning processes. Scholars analyzing legal standards in AI argue that applying conventional tests of negligence to algorithms is problematic because reasonable algorithmic behavior cannot be measured in the same manner as reasonable human behavior (Bashayreh et al., 2023). Machine learning models may generate emergent behaviors that were neither foreseeable nor intended, yet the mere occurrence of such behavior does not necessarily imply negligence. Analyses of AI regulatory concerns in telemedicine show that continuous updates to AI software create fluid conditions in which system behavior cannot be evaluated against fixed benchmarks (Ganapathy, 2021). These emerging patterns raise foundational questions about whether the standard of reasonableness should be recalibrated for digital actors or whether entirely new frameworks should be developed to accommodate the distinctive characteristics of algorithmic processes. The difficulty of establishing negligence for self-learning systems also challenges the theoretical coherence of tort doctrine, which traditionally relies on evaluating human actors and static products rather than evolving computational entities.

Attribution, one of the most fundamental components of tort analysis, becomes increasingly complex when harm arises from algorithmic systems. Tort law presupposes that responsibility can be allocated to specific actors—typically individuals or corporations—whose conduct produced the harm. However, algorithmic systems disrupt this paradigm by decentralizing agency across multiple stakeholders. Scholars examining legal personhood for AI systems argue that the ambiguous nature of AI agency complicates efforts to determine who should be held responsible for harmful outputs, especially when algorithms engage in autonomous decision-making that cannot be directly traced to human instruction (McDonald, 2023). Others examining AI in medical environments emphasize that attribution must consider not only designers but also data providers, clinicians, institutions, and regulators, since each contributes to the conditions under which harm arises (Cestonaro et al., 2023). The question of whether an autonomous system itself could be considered an "actor" for purposes of liability remains contested. While some scholars support limited forms of legal personality for AI to facilitate liability allocation (Gayvoronskaya & Galchun, 2021), others warn that attributing responsibility to machines risks shielding human actors from accountability. Because algorithms operate within socio-technical systems involving layers of human and machine contributions, doctrinal clarity about the identity of the tortfeasor remains elusive.

Vicarious liability introduces additional complications as organizations increasingly rely on algorithmic tools to perform functions traditionally carried out by employees or contractors. Under traditional doctrine, employers are liable for the torts of employees committed within the scope of employment. However, algorithmic systems are not employees, nor do they fit neatly into categories such as agents or independent contractors. Scholars analyzing the role of AI in professional settings note that organizations may delegate essential tasks—diagnostic interpretation, risk assessment, content moderation—to AI systems that act independently (Alyami et al., 2021). When errors occur, determining whether organizations should bear liability for the algorithm's actions becomes a central question. Analysts examining algorithmic harm in cultural and political systems argue that organizations benefiting from AI-driven operations must also bear responsibility for harms generated by their systems, even if those harms are not attributable to specific employees (Dyson, 2022). Yet courts may resist assigning vicarious liability when algorithms do not meet the doctrinal definition of an employee or agent. This doctrinal mismatch illustrates a broader challenge: algorithmic systems perform essential tasks but fall outside established relational categories that underpin vicarious liability.

Another significant doctrinal issue concerns whether algorithms should be treated as products, services, or a new class of digital agents. Product liability frameworks operate on the assumption that products are static objects whose defects can be evaluated based on design flaws, manufacturing errors, or inadequate warnings. However, machine learning systems evolve over time, potentially altering their behavior after deployment. Analyses of civil liability in medical AI contexts reveal that treating algorithms as traditional products is problematic because their capacity for self-modification undermines the stability required for product liability evaluation (Bączyk-Rozwadowska, 2022). Treating them as services introduces its own complexities, as services involve human performance rather than autonomous computational processes. Scholars studying revisions to European liability regimes emphasize that AI systems may require sui generis classification because they diverge from characteristics associated with both products and services (Gallese, 2022). Without clear doctrinal categorization, courts face difficulty determining whether strict liability, negligence, or hybrid standards should apply. Furthermore, service-based classifications may reduce opportunities for strict liability, thereby shifting burdens onto injured parties. This classification problem is one of the most important doctrinal challenges exposed by algorithmic harm.

Data quality and bias lie at the center of many algorithm-induced injuries, directly influencing how responsibility is conceptualized. Machine learning models depend heavily on training data, and defects in those datasets—whether resulting from incomplete representation, historical inequity, or systemic bias—can lead to harmful outcomes. Ethical analyses of AI systems emphasize that biased data can distort algorithmic judgments, particularly in healthcare, where inaccurate training sets can produce misdiagnoses or inequitable treatment recommendations (Elendu et al., 2023). Scholars addressing the use of AI in medical imaging also note that poor data governance can lead to algorithmic misinterpretation, underscoring the need for rigorous data-quality standards (Alyami et al., 2021). Defective data complicates legal responsibility because harms may originate not from the algorithm's computational processes but from the underlying dataset used to train it. Moreover, responsibility for data integrity may fall on different parties than those responsible for algorithm design. Analysts observing cybersecurity risks in healthcare highlight that data within digital ecosystems frequently passes through multiple actors, thereby making attribution and responsibility assessment even more difficult (Mosaddeque et al., 2022). When flawed or biased data leads to discriminatory or incorrect outputs, tort doctrine struggles to map responsibility onto the complex network of actors involved in data collection, curation, processing, and deployment.

Privacy also intersects with tort liability in algorithmic contexts, as data-driven systems rely on personal information to generate insights and predictions. Breaches of privacy can constitute independent harms, yet they can also serve as precursors to algorithmic injuries. Scholars examining AI deployment have noted that privacy violations may enhance the risk of downstream harms by introducing inaccuracies into data profiles or enabling malicious exploitation of personal data in automated systems (Tretyakova, 2021). These intertwined harms reveal that privacy is not merely an issue of information control but also a contributor to broader liability questions when algorithmic systems rely on compromised or misused data. Because tort law traditionally treats privacy and physical harms as distinct categories, the blending of these harms poses doctrinal questions about the scope and type of damages recoverable for algorithm-induced injuries.

Taken together, these conceptual and doctrinal challenges demonstrate that algorithm-induced harm exposes deep structural limitations within traditional tort frameworks. Algorithmic systems do not behave like human actors, nor do they function like conventional products or services. Their probabilistic, opaque, data-driven, and adaptive nature disrupts foundational principles of causation, reasonableness, attribution, and duty of care. As scholars analyzing AI ethics, liability, and regulatory structures have consistently emphasized, the complexity of digital ecosystems requires a reevaluation of tort doctrine rather than mere adaptation (Sqalli et al., 2023). The contradictions exposed by algorithmic harm reveal that tort law must confront an increasingly fragmented landscape in which responsibility is distributed across technological, institutional, and human contributors whose interactions challenge historical assumptions about agency, fault, and causation.

4. Comparative Legal Approaches and Emerging Regulatory Frameworks for Algorithm-Induced Harm

Legal systems across the world have responded to algorithm-induced harm through a wide range of regulatory approaches that reflect their underlying legal traditions, technological priorities, and sociopolitical contexts. The European Union has emerged as a leading actor in this domain, primarily through the development of the AI Act, which classifies AI systems based on risk and imposes stringent obligations on high-risk applications. Scholars examining civil liability for autonomous and robotic systems have noted that the EU framework emphasizes transparency, accountability, and rigorous oversight mechanisms intended to reduce harm before it occurs, with legal analyses underscoring the need for harmonized regulatory models capable of addressing the cross-border nature of algorithmic decision systems (Gallese, 2022). The EU's emphasis on stringent duty-of-care standards for developers and deployers aligns with broader trends in European civil liability discussions, including proposals to revise the Product Liability Directive to incorporate AI-specific considerations. Analyses of medical AI liability within European jurisdictions highlight that doctrinal flexibility is required to accommodate algorithmic transparency requirements, mandatory data quality controls, and prospective risk-management duties for operators of diagnostic tools (Cestonaro et al., 2023). Although the EU model attempts to provide clarity by placing structured obligations on high-risk AI providers, legal scholars caution that European frameworks may still struggle to resolve causal uncertainty, as flexibility in the evidence burden cannot entirely compensate for the opacity of complex learning architectures (Tretyakova, 2021). Nevertheless, the EU approach reflects a deliberate regulatory strategy aimed at mitigating algorithmic risks prior to deployment while expanding potential avenues for liability where risk-management duties are breached.

In contrast to the EU's comprehensive regulatory regime, the United States has approached algorithm-induced harm through a patchwork of tort doctrines, state-level regulations, and sector-specific initiatives. Observers of U.S. legal responses to autonomous-machine-caused injuries emphasize that American tort law continues to operate within traditional frameworks, such as negligence and strict liability, even while courts confront novel harms produced by automated systems (Huberman, 2020). The persistence of strong intermediary liability protections, especially those modeled on Section 230, complicates accountability for algorithmic amplification, content ranking, and automated moderation. Scholars studying generative AI in communication contexts note that U.S. immunity doctrines impede attempts to assign responsibility to platforms that deploy algorithms capable of amplifying harmful or misleading content (Zelinski, 2023). Debates surrounding algorithmic accountability bills reflect ongoing efforts to introduce transparency requirements or impact assessment obligations for automated decision systems, yet these legislative attempts remain fragmented across federal and state jurisdictions. Analysts of AI use in clinical and telemedicine contexts acknowledge that while the United States has seen rapid uptake of algorithmic tools, legal structures governing liability remain inconsistent across sectors, leading to uncertainties in professional responsibility and duty of care (Ganapathy, 2021). The U.S. model, therefore, illustrates the challenges of regulating algorithmic harm in a legal system that prioritizes decentralized governance and broad platform immunity, resulting in regulatory gaps that hinder effective doctrinal evolution.

The United Kingdom, Canada, and Australia adopt common-law approaches that integrate tort principles with statutory data protection regimes. Courts in these jurisdictions must navigate the interplay between privacy legislation, such as the UK Data Protection Act and Canada's PIPEDA, and traditional tort doctrines that address negligence, misrepresentation, and breach of statutory duty. Scholars examining AI's effect on civil liability within these systems highlight that data protection obligations can indirectly shape tort liability when misuse, misprocessing, or inadequate safeguarding of personal data leads to algorithmic injury (Kharitonova et al., 2022). In the UK, judicial reasoning shows increasing engagement with questions of foreseeability and standards of professional oversight as organizations deploy machine learning systems in sensitive domains, including healthcare and public administration. Analyses of the transformative impact of AI in biomedical and scientific research further suggest that these common-law systems must grapple with the blurred lines between professional judgment and automated recommendations, particularly as dependence on algorithmic support tools grows (Brogan, 2021). Canada faces similar challenges, with legal scholars highlighting the need to accommodate causation complexities in negligence claims involving diagnostic and predictive systems. Australian courts, meanwhile, have begun to recognize the systemic implications of biased or flawed datasets, reflecting academic concerns about how defective training data can produce discriminatory outcomes, as observed in healthcare-oriented discussions of AI ethics (Elendu et al., 2023). These systems demonstrate incremental adaptation within the common-law tradition, yet they still encounter conceptual barriers when attempting to map doctrinal principles onto algorithmic behavior.

Across Asia, regulatory frameworks for AI accountability are emerging rapidly, reflecting both governmental priorities and technological capabilities. China has introduced one of the most detailed regulatory regimes for algorithmic recommendation systems, focusing on transparency requirements, prohibitions against algorithmic discrimination, and obligations for platforms to prevent the amplification of harmful content. Scholars examining cybersecurity and digital system vulnerabilities underscore the relevance of these requirements in contexts where AI-driven detection and response systems must safeguard critical sectors such as healthcare, where algorithmic misjudgment can produce cascading harms (Mosaddeque et al., 2022). South Korea and Japan have also pursued AI governance frameworks that emphasize accountability for algorithmic outcomes, particularly in safety-critical contexts such as medicine and robotics. Commentators analyzing legal and regulatory structures for medical AI emphasize that Asian jurisdictions often integrate public health considerations into algorithmic accountability, recognizing the profound implications of automated decision-making in clinical settings (O'Sullivan et al., 2019). These frameworks highlight regional commitments to balancing innovation with protective safeguards, yet they also reveal gaps in liability allocation where algorithmic autonomy complicates causal analysis. The rapid pace of technological development in these jurisdictions often outstrips doctrinal adaptation, prompting ongoing debate about assigning responsibility among developers, operators, and institutions that deploy AI systems.

International soft-law instruments attempt to resolve cross-jurisdictional fragmentation by articulating normative principles for AI development, deployment, and oversight. The OECD AI Principles emphasize fairness, transparency, and accountability, which align with ethical concerns raised in discussions of AI in scientific and clinical environments (Alyami et al., 2021). The UNESCO AI Ethics Guidelines similarly promote risk-management approaches and safeguards against discrimination, echoing academic observations about biased training datasets and the risks they pose to vulnerable populations (Elendu et al., 2023). ISO standards for AI quality and safety management draw upon technical insights into algorithmic behavior, including predictive models used in healthcare diagnostics, reflecting concerns documented in analyses of diagnostic algorithm performance and system-level reliability (Cestonaro et al., 2023). While these soft-law frameworks do not impose binding obligations, they influence national regulatory agendas by offering coherent structures for addressing algorithmic risks. Scholars examining regulatory reforms for autonomous systems argue that these frameworks serve as conceptual scaffolding for legislative development, particularly in regions lacking mature AI governance infrastructures (Ganapathy, 2021). Despite their non-binding nature, international guidelines contribute to harmonization by providing shared terminology and generalizable principles for addressing algorithmic harm.

Comparative analysis reveals significant divergences in the allocation of burdens of proof and in the design of liability frameworks across jurisdictions. In the EU, proposals to invert burdens of proof for high-risk AI systems reflect scholarly recognition that plaintiffs face structural disadvantages when attempting to uncover algorithmic errors or establish causal chains within opaque systems (Tretyakova, 2021). Discussions of European liability reform highlight growing support for mandating insurance models for certain types of autonomous systems, echoing calls for preemptive compensation mechanisms in analyses of AI-related medical risks (Gallese, 2022). The EU focus on risk-based regulation contrasts sharply with the U.S. approach, where fragmented state-level oversight and persistent intermediary immunity protections limit the development of cohesive liability frameworks. Commentators caution that this regulatory inconsistency hinders efforts to assign responsibility for harms amplified by generative AI tools, particularly in contexts involving misinformation or biased recommendations (Zelinski, 2023). Meanwhile, common-law jurisdictions such as the UK, Canada, and Australia rely on traditional tort reasoning, yet their courts increasingly confront the doctrinal limits of foreseeability and reasonableness when evaluating harms caused by self-modifying or probabilistic systems. Analysts examining algorithmic integration into healthcare settings observe that these jurisdictions must reconcile statutory privacy protections with tort doctrines that were not designed to address the interplay between data misuse and algorithmic injury (Elendu et al., 2023).

Asian regulatory approaches tend to emphasize proactive oversight and administrative enforcement, particularly in China, where platform operators bear explicit duties to prevent discriminatory or harmful algorithmic behavior. Scholars studying cybersecurity frameworks in healthcare contexts point out that such regulatory models align with broader state interests in managing digital risk environments (Mosaddeque et al., 2022). South Korea and Japan incorporate safety-critical considerations into their emerging regulatory frameworks, integrating automated systems into long-standing risk-management traditions. While these systems provide clearer expectations for operators of algorithmic systems, scholars note that regulatory compliance does not necessarily resolve underlying doctrinal challenges related to causation or attribution, especially in sectors where algorithmic autonomy shapes decision-making (O'Sullivan et al., 2019).

International soft-law instruments attempt to resolve these divergences, yet the comparative landscape shows that national approaches remain largely unaligned. The OECD and UNESCO frameworks emphasize fairness, transparency, and accountability, echoing academic concerns about the ethical risks of autonomous and semi-autonomous systems, as articulated in discussions of biomedical research, algorithmic bias, and professional reliance on automated tools (Brogan, 2021). ISO standards attempt to supplement these high-level principles with technical guidance, mirroring the empirical focus of analyses examining how diagnostic algorithms behave in medical settings (Cestonaro et al., 2023). Despite their conceptual coherence, these instruments cannot overcome national differences in tort doctrine or regulatory philosophy. European systems favor ex-ante risk governance and structured obligations, the United States emphasizes decentralized liability and speech protections, common-law jurisdictions rely on judicial development of standards, and Asian systems often prioritize administrative control and platform responsibilities.

What emerges from this comparative landscape is a picture of legal systems attempting—sometimes effectively, sometimes inadequately—to resolve the conceptual gaps created by algorithmic autonomy, opacity, and adaptiveness. Scholars writing about AI liability, data ethics, cybersecurity systems, and automated decision-making repeatedly emphasize that algorithmic harm exposes fractures in foundational tort doctrines, making regulatory intervention necessary yet insufficient. European models attempt to compensate for doctrinal limitations through risk-based legislative mechanisms, while U.S. approaches rely more heavily on judicial reasoning and sector-specific regulation. Common-law countries integrate privacy protections and negligence doctrine but continue to face unresolved attribution and causation issues. Asian jurisdictions emphasize platform-level accountability but must still address the deeper conceptual challenges posed by dynamic and learning systems. International guidelines provide conceptual unity but lack binding authority.

These divergent approaches collectively demonstrate that algorithm-induced harm creates pressures that no single regulatory strategy has fully resolved. As algorithmic systems become more pervasive and autonomous, the comparative legal landscape reveals both the promise and limitations of regulatory frameworks in addressing the doctrinal contradictions discussed earlier in this review.

5. Conclusion

The evolution of cyber tort liability in the algorithmic era reflects a profound transformation in the way harm is produced, understood, and governed in contemporary societies. As digital ecosystems expand and autonomous systems increasingly shape social, economic, and professional environments, traditional legal doctrines face growing difficulty in responding to new categories of injury and responsibility. The preceding analysis illustrates that algorithm-induced harms do not merely represent an extension of earlier digital risks but instead signal a fundamental shift in the architecture of causation, agency, and accountability. These changes require a rethinking of tort principles that were developed in a world where human decision-makers, tangible products, and linear chains of causation served as the primary basis for liability.

At the heart of this transformation lies the challenge of opacity and complexity in algorithmic systems. Machine learning models, neural networks, and predictive algorithms operate through adaptive computational processes that escape straightforward explanation, making it difficult for injured parties to demonstrate how and why specific harms occurred. The inability to trace causal pathways undermines the utility of traditional evidentiary frameworks, which rely heavily on identifying direct connections between wrongful conduct and injury. When systems evolve autonomously or produce outputs based on statistical correlations that no human actor explicitly encoded, tort doctrines rooted in foreseeability and intentionality lose much of their relevance. This disconnect reveals a structural mismatch between the doctrinal foundations of tort law and the technological realities of modern automated decision systems.

Equally significant is the challenge of determining duty of care in digital environments characterized by distributed responsibilities. Algorithmic systems depend on the combined contributions of developers, data scientists, platform operators, institutional users, and end-users. Each plays a role in shaping how a system behaves, yet the boundaries of responsibility among these actors remain indistinct. Traditional notions of duty assume relatively clear roles and expectations, but digital ecosystems complicate these assumptions by diffusing accountability across networks of actors who may never interact directly. This diffusion challenges both the conceptual coherence of duty and the practical enforceability of tort-based remedies.

The standard of reasonableness, a cornerstone of negligence doctrine, also faces structural strain when applied to algorithmic conduct. Reasonableness is historically grounded in human capacities, norms, and moral expectations. Autonomous systems, however, do not reason or act according to human logic, nor do they respond predictably to changing contexts. Their capacity for self-adjustment creates evolving behavioral patterns that defy static evaluations of reasonable conduct. As a result, courts may struggle to assess whether a system’s behavior falls within an acceptable range of outcomes or whether deviations constitute negligence. Without reliable benchmarks for evaluating algorithmic behavior, the negligence framework risks becoming either overly permissive or arbitrarily punitive.

Attribution, another foundational element of tort liability, becomes elusive when harms arise from interactions between humans and autonomous systems. The question of who—or what—should bear responsibility for algorithm-induced injury exposes deep conceptual tensions. Attributing responsibility to developers alone ignores the role of operators and data curators; attributing it to institutions may obscure the technical mechanisms that produce harm; attributing it to the algorithm itself risks displacing human accountability onto non-human entities. This ambiguity reveals the inadequacy of tort doctrines premised on singular agents and discrete acts. Algorithmic harms are inherently systemic, arising from complex interactions across technological and organizational layers, and tort law has yet to identify a coherent method for capturing this complexity.

The complications surrounding vicarious liability highlight a related tension. Organizations increasingly rely on automated systems to perform functions once executed by human employees, but these systems do not fit neatly within established categories such as servants, agents, or independent contractors. If an organization benefits from an algorithm’s operations, it may seem intuitive to hold it responsible for algorithmic harms. However, absent clear doctrinal grounding, courts may hesitate to extend vicarious liability to autonomous systems, particularly when system behavior is unpredictable or not fully understood. This uncertainty weakens incentives for organizations to implement robust oversight mechanisms and creates gaps in protection for individuals harmed by automated processes.

The debate over whether algorithms should be treated as products, services, or a distinct category of digital agents further demonstrates the conceptual challenges at the core of cyber tort liability. Product liability assumes that products are stable and unchanging, yet adaptive systems defy this assumption. Treating algorithms as services may offer theoretical clarity but fails to reflect their autonomous operational capacity. The difficulty of classification reveals a deeper issue: algorithmic systems blur boundaries between objects and actors, making them incompatible with rigid doctrinal categories. Without resolving this classification problem, tort law cannot consistently determine when strict liability applies or what duties accompany the creation and deployment of autonomous systems.

Compounding these doctrinal challenges are the pervasive issues of data quality, privacy, and bias. Algorithmic systems depend on data that may be incomplete, inaccurate, or embedded with historical inequities. Harms arising from biased or defective data complicate responsibility because they originate not from the algorithm’s computational functions but from systemic shortcomings in data collection and governance. Privacy violations similarly contribute to downstream harms by enabling misuse or misinterpretation of sensitive information. These interconnected harms challenge tort law to address not only the immediate injury but also the structural conditions that make algorithmic harm possible.

Across jurisdictions, regulatory responses have attempted to compensate for the limitations of tort doctrine, but these efforts vary widely in effectiveness and coherence. The EU has adopted a risk-based, preventative model emphasizing transparency and oversight, while the United States relies more heavily on traditional tort frameworks, sectoral regulation, and platform immunity. Common-law jurisdictions integrate data protection with negligence, yet they still struggle with causation and foreseeability. Asian jurisdictions emphasize administrative control and platform responsibility, but doctrinal challenges persist. International soft-law principles offer conceptual guidance but lack binding force. This fragmentation reflects both the novelty of algorithmic harms and the absence of consensus on how liability should evolve.

Taken together, these findings show that algorithm-induced harm exposes deep structural limitations in existing tort doctrines. The assumptions that once anchored liability—human agency, foreseeability, direct causation, stable products, and organizational oversight—no longer map neatly onto digital ecosystems shaped by autonomous and adaptive systems. As a result, tort law faces a pivotal moment of transformation. Future legal frameworks must grapple with the reality that harm is increasingly produced by systems that defy conventional categories, that responsibility is distributed across networks rather than centered on individuals, and that injuries may arise from informational or structural failures rather than discrete acts.

The conclusion reached through this analysis is that the evolution of cyber tort liability requires not only doctrinal adaptation but conceptual innovation. Algorithmic systems challenge the very foundation of tort law, demanding new ways of understanding agency, accountability, and harm. Without rethinking these core concepts, legal systems will remain ill-equipped to protect individuals, regulate technology, and promote responsible innovation in an era defined by autonomous decision-making.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Alyami, A. S., Majrashi, N. A., & Shubayr, N. A. (2021). Radiologists' and Radiographers' Perspectives on Artificial Intelligence in Medical Imaging in Saudi Arabia (Preprint). https://doi.org/10.2196/preprints.35765

Bączyk-Rozwadowska, K. (2022). Civil Liability for Damages Caused in Connection With the Use of Artificial Intelligence in Medicine. *PPM*, *3*(3-4), 5-35. https://doi.org/10.70537/z7xnk378

Bashayreh, M. H., Tabbara, A., & Sibai, F. N. (2023). The Need for a Legal Standard of Care in the AI Environment. *Sriwijaya Law Review*, 73-86. https://doi.org/10.28946/slrev.vol7.iss1.1507.pp73-86

Brogan, J. (2021). The Next Era of Biomedical Research. *Voices in Bioethics*, *7*. https://doi.org/10.52214/vib.v7i.8854

Cestonaro, C., Delicati, A., Marcante, B., Caenazzo, L., & Tozzo, P. (2023). Defining Medical Liability When Artificial Intelligence Is Applied on Diagnostic Algorithms: A Systematic Review. *Frontiers in Medicine*, *10*. https://doi.org/10.3389/fmed.2023.1305756

Chagal-Feferkorn, K. (2021). How Can I Tell if My Algorithm Was Reasonable? *Michigan Technology Law Review*(27.2), 213. https://doi.org/10.36645/mtlr.27.2.how

Dyson, M. R. (2022). Combatting AI's Protectionism &Amp; Totalitarian-Coded Hypnosis: The Case for AI Reparations &Amp; Antitrust Remedies in the Ecology of Collective Self-Determination. *Smu Law Review*, *75*(3), 625. https://doi.org/10.25172/smulr.75.3.7

Elendu, C., Amaechi, D. C., Elendu, T. C., Jingwa, K. A., Okoye, O. K., Okah, M. J., Ladele, J. A., Farah, A. H., & Alimi, H. A. (2023). Ethical Implications of AI and Robotics in Healthcare: A Review. *Medicine*, *102*(50), e36671. https://doi.org/10.1097/md.0000000000036671

Gallese, C. (2022). Suggestions for a Revision of the European Smart Robot Liability Regime. *Icair*, *4*(1), 29-35. https://doi.org/10.34190/icair.4.1.851

Ganapathy, K. (2021). Artificial Intelligence and Healthcare Regulatory and Legal Concerns. *Telehealth and Medicine Today*. https://doi.org/10.30953/tmt.v6.252

Gayvoronskaya, Y., & Galchun, E. A. (2021). The Harm Caused by Artificial Intelligence: Aspects of Responsibility and Legal Personality. *Advances in Law Studies*, *9*(4), 76-80. https://doi.org/10.29039/2409-5087-2021-9-4-76-80

Huberman, P. (2020). Tort Law, Corrective Justice and the Problem of Autonomous-Machine-Caused Harm. *Canadian Journal of Law & Jurisprudence*, *34*(1), 105-147. https://doi.org/10.1017/cjlj.2020.3

Kharitonova, Y. S., Savina, V., & Pagnini, F. (2022). Civil Liability in the Development and Application of Artificial Intelligence and Robotic Systems: Basic Approaches. *Вестник Пермского Университета Юридические Науки*(4(58)), 683-708. https://doi.org/10.17072/1995-4190-2022-58-683-708

McDonald, L. (2023). AI Systems and Liability: An Assessment of the Applicability of Strict Liability &Amp; A Case for Limited Legal Personhood for AI. *St Andrews Law Journal*, *3*(1), 5-21. https://doi.org/10.15664/stalj.v3i1.2645

Moodley, K. (2023). Artificial Intelligence (AI) or Augmented Intelligence? How Big Data and AI Are Transforming Healthcare: Challenges and Opportunities. *South African Medical Journal*, *114*(1), 22-26. https://doi.org/10.7196/samj.2024.v114i1.1631

Mosaddeque, A., Rowshon, M., Ahmed, T., Twaha, U., & Babu, B. N. (2022). The Role of AI and Machine Learning in Fortifying Cybersecurity Systems in the US Healthcare Industry. *Ijss*, *1*(2), 70-81. https://doi.org/10.63544/ijss.v1i2.101

O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Léonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019). Legal, Regulatory, and Ethical Frameworks for Development of Standards in Artificial Intelligence (AI) and Autonomous Robotic Surgery. *International Journal of Medical Robotics and Computer Assisted Surgery*, *15*(1). https://doi.org/10.1002/rcs.1968

Sqalli, M. T., Aslonov, B., Gafurov, M., & Nurmatov, S. (2023). Humanizing AI in Medical Training: Ethical Framework for Responsible Design. *Frontiers in Artificial Intelligence*, *6*. https://doi.org/10.3389/frai.2023.1189914

Tretyakova, E. P. (2021). Using Artificial Intelligence in Healthcare: Allocating Liability and Risks. *Digital Law Journal*, *2*(4), 51-60. https://doi.org/10.38044/2686-9136-2021-2-4-51-60

Zelinski, C. (2023). Chatbots, Generative Ai, and Scholarly Manuscripts Wame Recommendations on Chatbots and Generative Artificial Intelligence in Relation to Scholarly Publications. *Journal of Postgraduate Medical Institute*, *37*(3), 221-224. https://doi.org/10.54079/jpmi.37.3.3284