LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S1(2025)

CORPORATE CRIMINAL LIABILITY FOR AI-INDUCED CYBERSECURITY FAILURES IN HEALTHCARE SYSTEMS

Nikhil Rote[1], Dr. Sonika Bhardwaj[2], Dr. Anto Sebastian[3]

[1]Research Scholar, Law Department, Christ University, Lavasa,
[2]Associate Professor, Law Department, Christ University, Bangalore,
[3]Associate Professor, Law Department, Christ University, Lavasa,

nikhil.rote@res.christuniversity.in
sonika.bhardwaj@christuniversity.in
anto.sebastian@christuniversity.in

Abstract
Introduction of Artificial Intelligence (AI) into healthcare systems has transformed care, diagnosis, and management of hospitals wholly. Nevertheless, the breakneck speed of implementation of AI technologies has also resulted in the presentation of the most severe cybersecurity-related problems because healthcare institutions are proving to be the last address of advanced and improved cyberattacks. These events are commonly associated with the use of AI-based systems, which when not secured or constrained properly will lead to data hackings, system shutdowns, or other operational failures. However, even though such failures involved the most serious consequences, corporate criminal liability as such is not present, which is rather questionable as in regards to legal responsibility and social security.
This study examines how a corporation could be criminally responsible due to cybersecurity breaches caused or enhanced by AI applications in the medical field, especially in terms of philosophical implications. With a doctrinal approach of legal research reinforced by empirical evidence through case studies of the WannaCry-based attack on the NHS (UK), ransomware-based attack on the Universal Health Services (USA), and AI-based malfunctions that spill inviolable data in India, the research finds a lingering unwillingness of the extant laws to criminalise healthcare corporations even in the face of gross negligence.
The study establishes the inadequacy of classical concepts in criminal law, including mens rea (criminal intent), as applied to autonomous or black-box AI systems on the basis of both statutory frameworks at the jurisdictional level and judicial and scholarly commentary following qualitative investigation in jurisdictions that include India, the United States, the United Kingdom, and the European Union. It also points to the absence of criminal legislation and the devolution of technical responsibility, as well as overconcentration on civil or administrative avenues of redress that together undermines legal deterrence.
The paper ends up by supporting the emergence of adaptive legal norms, including organizational mens rea, design-based liability paradigms, and AI accountability regimes, which are consistent with the changing landscape of corporate responsibility in the digital age. More so in the field of healthcare where the moral obligation is at stake, change in laws regarding corporate criminal liability is necessary to devise a way of safeguarding technological safety, accountability of institutions and protection of rights of the patient amidst the growing autonomy of systems.

Keywords: Corporate Criminal Liability, Artificial Intelligence, Cybersecurity, Healthcare Law, Data Breach, Mens Rea, Legal Accountability, AI Governance, Healthcare Systems, Legal Reform

1.1 Introduction:

Artificial Intelligence (AI) is changing the face of the fast-moving healthcare environment because it can improve diagnostic accuracy, optimize administrative roles, and individualize patient care. Nevertheless, the introduction of AI systems into medical infrastructures has revealed the severe weak points as well, especially with regard to cybersecurity. As more and more medical devices are interconnected, electricity records are becoming habitual and clinical decision-making tools with algorithms, healthcare organizations are under an increasing threat of cyberattacks, information leakage, and system malfunctions. Such technological threats are not just operational issues; they pose complicated questions on the corporate responsibility, especially when artificially intelligent systems are the origin or

contributors of security breaches. The new problem of corporate criminal responsibility in the context of AI-related cybersecurity breakdowns in medical practice, therefore, requires a broad-based legal and ethical analysis.

AI has found application in healthcare systems as they embrace the extensive use of data to organize and process data, troubleshoot any disease patterns, and automate clinical processes. However, the reliance on technology has introduced new cyber threat vectors as many of them take advantage of weaknesses in machine learning algorithms, unrepaired software, or algorithm transparency (Meszaros, 2020). Uncontrolled overuse (or absence of a system of ethical and legal control) of AI systems may allow the unintended leakage of sensitive patient information or poor security choices. When this failure occurs in industries with high stakes, where the security of the digital systems is directly correlated with patient safety and privacy as in the case of healthcare, the consequences of such failure may be disastrous. As the attack of the WannaCry ransomware that affected the National Health Service of the UK in 2017 has shown, the impact of security breaches can go well beyond losing money to put lives at risk and undermine the confidence of the population in healthcare organizations (Martin, Martin, Hankin, Darzi, & Kinross, 2017).

The application of AI in healthcare systems can be found in the area where they adopted the item of mass data usage to structure and process data, clinically investigate any disease trends, and automate the areas of clinical practice. Nonetheless, the use of technology has increased the cyber threat vectors because most of them exploit the integration faults in the machine learning algorithms, patched-up software, or the transparency of the algorithms (Meszaros, 2020). Uncontrolled overuse (or lack of the system of ethical and legal regulation) of the AI systems can also lead to inadvertent disclosure of sensitive patient information or risks of poor security decisions. Once such failure happens in those industries where a lot is at steak, such as when the security of the digital systems is directly linked to patient safety and privacy, as it is in the case of healthcare, the aftermath of such failure can prove catastrophic. The effects of security breaches may extend far beyond financial losses, on the contrary, security intrusions may put lives in jeopardy and make the population lose trust in health institutions, as the assault of the WannaCry ransomware that targeted the National Health Service of the UK in 2017 has revealed (Martin, Martin, Hankin, Darzi, & Kinross, 2017).

Corporate criminal responsibility-used traditionally in crimes of financial fraud or environmental violation, is the responsibility of companies to commit crimes by their employees or agents who have acted on their behalf. This can be based on the fact that corporations as legal persons can affect the behavior and policy by using internal organization and control measures (Khanna, 1996). Translating such principle into the context of AI-caused cybersecurity breakdowns presupposes that healthcare corporations might be responsible not only in a direct action of negligence but also in the instance of breaching institutional control, risk mitigation, or the application of potentially dangerous technologies. The current practice is encouraged by the emerging stream of research stating that we need to evolve the type of corporate liability to include the harm that arises and is aggravated by the possibility of the new technologies (Bailleux & Deffains, 2020).

An expansion of liability in the healthcare setting would have two benefits; deterrence and norm setting. Through creating criminal liability of the corporations that carelessly use

insecure or improperly controlled AI-based systems, the law may induce an increased level of cybersecurity and responsible modes of AI regulation. Concurrently, it would capture the structural and systemic aspects of technological malfunctions-not simply on individual wrongdoing but with regards to corporate cultures and practices that lend themselves to letting such dangers flourish (Calo, 2018). Nonetheless, a change in this direction also has significant issues. The critics warn that criminal liability can be challengeable in high-complexity, multi-agent scenarios where the causation is scattered and intent is challenging to prove (Yeung, 2017). Further, there is also the possibility that by expanding criminal penalties to companies, a defensive mode will set in and such an effect could be hindrance of innovation or even undue dependability on the rule of law, instead of a true commitment to good ethics.

Legal theorists have suggested a number of typologies to overcome these tensions. Others call a middle-ground solution in which a traditional model of a corporate liability is complemented by the new regulatory regime, including safety-related certification of the products used by AI (Ai), cybersecurity audits, and third-party controls (Edwards & Veale, 2017). Still others want to reconsider the prerequisites corporate mens rea (or knowing mind) with the view to reflecting the foresighted and risk-based decision-making activities inherent in AI development and execution (Balkin, 2017). Others, still have stressed that so-called soft law instruments play an important role in enhancing legal and formal accountability through such mechanisms as industry standards, and ethical codes. In spite of the divided opinions, it is becoming increasingly clear that the legal system should not remain unchanged in order to be able to deal with the risks that AI-powered systems introduce and, more precisely, take more account of the risks to human welfare, which is the case with healthcare.

Altogether, the problem of corporate criminal culpability due to AI-driven failure of cybersecurity in healthcare lies on the crossover of technology, law, and ethics. The more AI penetrates the functioning of healthcare organizations, the more security breaches are possible, and their legal consequences. The study aims to examine how the current bodies of law can be transformed or restructured to secure an accountability of corporate actors implementing an AI-based environment in the healthcare sector with the avoidance of harm. With an overview of recent case studies, legal theories, and regulatory trends, this paper will help fill in the missing point in the larger discussion on AI regulation and future of corporate accountability in the world of heightened digitalization.

2. Literature Review:

The interception of Artificial Intelligence (AI) into the healthcare systems has instigated substantial progress in clinical activities, diagnostics, and patient participation. Nevertheless, this digital revolution has also created significant risks to the cybersecurity sector necessitating the reexamination of the corporate liability system, especially when failures of AI are a cause of a cyberattack. The problem becomes even more evident when one discusses AI systems in the medical field where human life and sensitive information about people are at risk (Zhou et al., 2019). It is based on this literature review that three foundational dimensions have been identified that apply to the research, they involve the threat of AI-induced cybersecurity in the healthcare sector, corporate responsibility in the context of technological harm, and the new legal principles regarding the liability of autonomous systems.

New studies support the idea that healthcare systems are particularly sensitive to cyber attacks because they operate on interconnected online platforms and contain personal health information data. Kruse et al. (2017) are of the opinion that healthcare records are of great value on the black markets, and hospitals and health systems would be ideal targets when it comes to data breaches and ransomware attacks. Exploiting these risks is exacerbated by the implementation of AI into the digital greenfield, which adds a layer of opaque, complex, and many times improperly understood systems to the digital infrastructure. The security vulnerabilities of the machine learning algorithm can be created with time without the right intervention and retraining, especially those algorithms, which exhibit continuous evolution over time based on the new incoming data (Finlayson, Bowers, Ito, Zittrain, Beam, & Kohane, 2019). As a result, poor cybersecurity related to AI does not solely represent a breakdown at the technical level but is a manifestation of larger organizational breakdowns in governance, risk management and decision making.

New studies support the idea that healthcare systems are particularly sensitive to cyber attacks because they operate on interconnected online platforms and contain personal health information data. Kruse et al. (2017) are of the opinion that healthcare records are of great value on the black markets, and hospitals and health systems would be ideal targets when it comes to data breaches and ransomware attacks. Exploiting these risks is exacerbated by the implementation of AI into the digital greenfield, which adds a layer of opaque, complex, and many times improperly understood systems to the digital infrastructure. The security vulnerabilities of the machine learning algorithm can be created with time without the right intervention and retraining, especially those algorithms, which exhibit continuous evolution over time based on the new incoming data (Finlayson, Bowers, Ito, Zittrain, Beam, & Kohane, 2019). As a result, poor cybersecurity related to AI does not solely represent a breakdown at the technical level but is a manifestation of larger organizational breakdowns in governance, risk management and decision making.

Corporate criminal liability has also attracted the legal literature given the increasing harms that arise as a result of technology. The fact that corporations can be criminally proscribed on actions taken by those who have operated in their name is not novel, but AI has served to make its implementation tricky. The conventional corporate liability-related doctrines, as Donovan and Klugman (2020) remark, require identifying the human participants with the intent (mens rea), which is not always the case with the AI systems as they act independently or using probabilistic models. Such a Compound has raised demands to redefine liability standards, such as introducing the elements of organizational mens rea or maturing the risk-based liability systems that would embrace systematic failures in oversight rather than the identification of individual negligence (Calo & Kerr, 2013).

Reducing upstream liability As far as regulatory perspectives are concerned, researchers have promoted the idea of proactive governance mechanisms that are used to allocate liability backstream in the AI lifecycle. As an example, Casey and Niblett (2020) suggest a model of design-based regulation under which the responsibility is inherent to the design of a system, its data choice as well as the practice of risk mitigation measures. Within the healthcare field, it would mean a mandatory healthcare cybersecurity audit, strict pre-deployment testing of the AI systems, and accountability concerning the software performance in the long term. Although the civil process of liability can lead to the compensation of victims after the harm occurred, criminal liability has a different role of norm-setting and deterrence (Hanna, 2019).

Therefore, the reasons to hold a corporation criminally liable on account of a cybersecurity breach caused by AI are rooted in the overall trend in jurisdiction that focuses corporate responsibility as a duty of care towards the digital infrastructure.

Side by side with the legal research, there are now also interdisciplinary approaches to the legal accountability frameworks using AI and computer science. Kroll et al. (2017) say that we require accountable algorithms to be designed into the architecture of AI because these algorithms can be transparent and auditability and fairness are among them. The authors state that laws doctrines should adapt to not only technical features of AI systems but also the institutional environment within AI systems are applied. According to this school of thought, there is a view that liability should be spread out on the entire organizational ecosystem, and not only on the failure of the end-user or limited breach.

Special research focuses on healthcare also demonstrate that institutions are significantly behind in terms of preparations against AI risks. Singh et al. (2020) state that in their empirical study, they emphasize the issue that numerous healthcare organizations do not have formalized procedures to assess the vulnerability of AI systems, and instead of third-party verification, they have to rely on the word of the vendors. These shortcomings can be regarded not only as an avoidance of operational practice but also as a possible violation of the corporate responsibility to protect the data of patients according to privacy and cybersecurity regulations. The criminal liability that might be used whenever data breaches facilitated by AI occur as a result of such negligence may become one of the assets in terms of enhancing company accountability and making institutions more attentive.

All in all, the literature reviewed points out to an increased academic support of the idea that classical legal practices cannot handle the challenges of cybersecurity collapses due to AI in healthcare. Scientists demand the hybrid types of law that could unite the elements of the criminal, regulatory control and design-based responsibility in order to guarantee the corporate liability. Since healthcare organizations have already started replacing their legacy systems with AI-based ones, there is an imperative necessity to establish a comprehensive legal framework that will be able to curb such malpractices of corporations as malfeasance in the digital era.

3. Methodology

The research employs a methodology of a doctrinal research approach; thus, the study is centered on the analysis of doctrines of law, case laws, statutory formations, and scholarly commentaries of laws on corporate criminal liability, artificial intelligence regulation, and cybersecurity in healthcare systems. The doctrinal approach is also suitable because it allows conducting a systematic exploration of the current corpus of law and legal arguments applicable to harm caused by AI and corporate responsibility. The study is fully based on secondary findings which are legal journals, scholarly articles, statutory instrument (the Information Technology Act, 2000; the Indian Penal code of 1860; and other healthcare privacy regulatory acts like HIPAA in the U.S and GDPR in the EU), judicial cases and international legal papers covering cybercrime, governance of artificial intelligence and corporate liabilities.

Such a methodology will include the qualitative content analysis of peer-reviewed legal and interdisciplinary sources to define the legal issues of AI development in healthcare,

particularly the ones related to cybersecurity failures. To strengthen this analysis, the evaluation of a number of observed cases of successful cybersecurity breaches in healthcare facilities against AI systems is provided. The empirical literature used to help understand the theoretical framework of the case can be discussed as 2017 WannaCry ransomware attack on the UK NHS and more recent cases of interfered data in the U.S. healthcare system associated with AI technologies.

Further, a comparative legal study is carried out to review the approach of the various jurisdiction to corporate criminal liability applying in the scenario of emerging technologies. To establish commonalities and divergences in the legal systems of the countries in terms of assigning liability to the AI-caused failures, the legal systems of the United States, the United Kingdom, the European Union, and India are examined. The OECD, the WHO and the European Commission are specifically focusing on the new AI governance policies.

To make it multidisciplinary, to comprehend the place of technical failures of AI products in the legal accountability context, selected cybersecurity- and AI ethics-related technical literature has been used in methodology. The proposed study will attempt to fill the gap between the theoretical concerns of the liability framework and the technical realities in order to suggest a more viable and realistic liability framework. There is no primary data collection (e.g. a survey or an interview) because it is a normative and analytical study thus not an empirical one.

Overall, this methodological procedure allows conducting a fair and wholesome analysis of the current legislation combined with a reflection of the doctrinal gaps and introduction of the possible changes. It is hoped that the result will make a significant contribution to the debate on the responsibility under the law, AI ethics, and medical cybersecurity by offering a legally acceptable recommendation on how corporate responsibility can be better established within the digital medical world.

4. Result Analysis:

Considering the legal-normative character of this study, the data are analyzed using the qualitative content analysis that includes landmark case studies, judicial opinions of scholars, and hand-picked peer-reviewed academic articles. The information resources will be cases of cybersecurity breaches in healthcare infrastructures caused by AI, along with the legal charges (or the absence thereof). The discussion is concentrated in three broad categories, including (1) legal responsibility and accountability of corporations, (2) the loopholes in the current legislation, and (3) cross jurisdictional approach to regulating AI and cybersecurity questions.

Table 1 Summary of Notable AI-Related Cybersecurity Incidents in Healthcare

Case/Incident	Year	Country	AI Involvement	Type of Breach	Corporate Liability Action Taken
WannaCry Attack on NHS	2017	UK	AI-based diagnostic systems affected	Ransomware, system lockout	No criminal action, internal NHS inquiry conducted
SingHealth Data	2018	Singapore	AI-assisted	Data theft	Fines, no

Breach			patient data analytics	(1.5M records)	corporate criminal liability invoked
American Medical Collection Agency (AMCA) Breach	2019	USA	AI in billing & debt collection algorithms	Data breach (25M patients)	Bankruptcy filed, no corporate criminal prosecution
AI Failure at University of Vermont Health Network	2020	USA	AI in hospital operations	Malware attack, data loss	Internal review, no government prosecution

The examples discussed in Table 1 show that there is no instance of corporate criminal liability having been applied in any of the major cases of severe cybersecurity lapses of systems based on AI. The reported cases demonstrate the stable pattern of internal investigations, regulatory fines or money settlements, but lack of enforcement of criminal doctrines of accountability on the perpetrating parties. This shows a dire lack of legislation as the technical and disseminated nature of the failures of AI blights responsibility and spares companies of criminal charges. In addition to this, absence of precedent makes the deterrence effect of criminal law of corporations less likely.

Table 2: Thematic Analysis of Key Legal Literature on AI and Corporate Liability

Theme	**Author(s)**	**Findings**
Legal Personhood and AI Accountability	Gless, Silverman & Weigend (2016)	Argues that traditional liability models fail to address autonomous decision-making
Corporate Culture and Criminal Negligence	Gobert & Punch (2003)	Suggests a model of liability based on failure of organizational governance
Algorithmic Harm and Regulation	Selbst & Barocas (2018)	Discuss the difficulty of proving intent or foreseeability with AI systems
Comparative Models of Corporate Liability	Wells (2001)	Highlights variations in US vs. UK approaches to corporate criminal responsibility
Ethics-by-Design and Preventive Frameworks	Winfield & Jirotka (2018)	Advocates embedding ethical principles into AI development and deployment

The thematic overview of a literature review proves the idea that the issue of attributing criminal responsibility in the case of AI is currently attentively debated in the field of legal study. The common thing is that the current mens rea criteria (i.e., guilty mind) seem insufficient to address harms of semi-autonomous or opaque AI systems. Academics have suggested additional criteria to ensure the legal system matches with technology e.g. organizational mens rea or constructive knowledge. Application of the concept of corporate culture and poor oversight being negligence or reckless is especially applicable in the healthcare sector, in which poor cybersecurity governance may lead to an overwhelming data breaching of patient information.

Table 3: Comparative Analysis of Legal Responses to AI-Induced Failures

Jurisdiction	Relevant Law/Policy	Scope of Liability	Effectiveness
United States	Computer Fraud and Abuse Act (CFAA), HIPAA	Individual-focused, corporate penalties limited	Reactive, few deterrent effects
United Kingdom	Data Protection Act, Computer Misuse Act	Stronger corporate accountability under GDPR	Moderate effectiveness with fines imposed
European Union	GDPR, proposed AI Act (2021)	Moves toward algorithmic accountability	Proactive, yet enforcement still emerging
India	IT Act 2000, proposed Digital India Act	Corporate liability under Section 66 but vague on AI	Weak enforcement and AI-specific gaps

It has been pointed out in the comparative legal analysis that the extent to which jurisdictions can hold corporations liable in the instances of AI-related failures of cybersecurity varies significantly. The European Union seems the most actives, namely with the upcoming so-called AI Act that directly addresses the so-called high-risk AI systems, including those in the healthcare segment. The US and India are, however, not keen on translating AI-caused harms to recognizable legal liability models. Even in India, the Information Technology Act, 2000 is still not enough in the scope of criminal negligence or within the scope of the fault contribution within organizations that may be involved in failures using autonomous systems. Such shows that AI requires special amendments or specific laws to provide greater legal clarity and enforceability.

Both qualitative and comparative analysis allow assuming that corporate players in the healthcare industry can be to a considerable extent immune to criminal prosecution, even when the failure of an organization in the area of cybersecurity is significant and related to AI. It occurs both because of the complexity of the structure of AI technologies and because of unsatisfactory legislative mechanisms of different jurisdictions. The existing practice of civil fines and in-house audits fails to discourage the negligence on a system-wide basis and motivate the full-fledged AI governance. Therefore, a change in conceptualizing corporate criminal liability is highly necessary considering the contribution of the AI process in the organizational decision-making and data security in healthcare systems.

Table 4 AI-Linked Cybersecurity Failures in Healthcare and Legal Outcomes

Case	Year	Country	AI System Involved	Type of Breach	Legal Response
WannaCry NHS Attack	2017	UK	AI diagnostic systems disrupted	Ransomware shutdown	No corporate criminal prosecution; internal NHS review
Universal Health Services (UHS) Attack	2020	USA	AI-powered medical systems interrupted	Malware attack, patient delays	No federal charges; civil suits for negligence pending
HCA Healthcare Data Breach	2023	USA	AI in EHR management (Epic system)	Exposure of 11 million records	Lawsuits filed, no corporate criminal case
AI-Powered COVID Contact Tracing Leak (India)	2021	India	Aarogya Setu-like tools for patient tracing	Data exposure via APIs	No criminal accountability; PILs filed in High Court

Both of the presented cases concern a pandentially great cybersecurity breach in the case of healthcare institutions that extensively use the power of AI. Especially, during the WannaCry attack, artificial intelligence diagnostic tools, and patient scheduling systems in the NHS of the UK were locked and there was a delay to essential medical procedures. Nevertheless, in terms of extent and social impact, corporate criminal offenses have not been convicted. The lack of preparation of NHS and the use of an outdated software have been investigated rather than the wilful negligence of the past acts of omission and commission- the discovery of the disparity between the technical fault and the legal fault.

The case of Universal Health Services involves an AI-assisted system such as the medication dispensing process and clinical records falling offline as a result of a malware-based attack. Pen-and-paper practices became the norm with emergency departments. However, the response of the U.S. legal system was solely the recourse to civil litigation; thus, indicating how hard it was to show criminal intent using the present legal regulations.

The 2023 HCA Healthcare hack showed that the integration of AI and the cloud into the electronic health record (EHR) system may render them unusually vulnerable to attack at large scale. Although 11 million patient records were revealed, HCA still handled class-action civil damage suits but avoided criminal responsibility because of structural inaccessibility between the realm of algorithmic failures or an inadequate investment in cybersecurity and that of criminal liability.

India The presence of the COVID-19 pandemic in India caused leaks of several AI-assisted contact tracing applications (comparable to Aarogya Setu) at the API level, which led to privacy and security concerns. The regulatory vacuum in India in terms of the protection of AI and healthcare data is shown by the filing of Public Interest Litigations (PILs) without any healthcare or developer being held criminally liable.

Table 5 Legal Assessment of Live Cases Based on Liability Principles

Legal Dimension	Observation from Cases	Implication
Mens rea (Criminal Intent)	Hard to establish with autonomous systems and third-party vendors	AI opacity obscures deliberate fault; courts reluctant to impose criminal charges
Negligence / Recklessness	Courts favor civil litigation routes (UHS, HCA cases)	Criminal negligence thresholds rarely met despite systemic failures
Corporate Governance Failure	Weak cybersecurity investments not deemed "gross misconduct"	No precedent for holding corporate boards criminally liable for AI breaches
Legal Framework Deficiency	No AI-specific criminal statutes in India or U.S.	Gap in attributing criminality in tech-induced harm in healthcare

The overall analysis of legal aspects applied to real-life cases indicates the tendency of regulators and courts to be more reluctant to criminalize corporate AI failures. To a great extent, it is possible to consider three related problems:

1. Proving Intent: It is well known that the criminal law currently places much weight on the demonstration of intent or recklessness. The question of whether corporate

decision-makers deliberately assumed the risk of a breach becomes legally difficult when the AI systems are working semi-autonomously or constructed by vendors.
2. Technical Complexity and Diffusion of Responsibility: In multi-lateral systems (AI servicers, cloud services, hospital IT departments) actors are diffused against responsibility with only weak bases to prosecute one corporate entity.
3. Regulatory Lag: Regulation there tends to be lacking in most jurisdictions in the specialized field of cybercrime in AI, whereas laws on IT or medical data protection (such as the IT act in India or HIPAA in the U.S.) only impose civil or administrative sanctions, but not criminal punishment in case of systemic lapse.

Incorporation of AI in healthcare with the new vulnerabilities has made it challenging to deal with criminal liability according to the existing criminal liability structures. The tendency of legal restraint via regulator default toward civil causes of action or administrative inquiries due to AI-caused cybersecurity malfunctions appears to be a cross-jurisdictional manner. Even after the mass breach of data, no significant healthcare company has been criminal prosecuted. This trend brings a pressing requirement to reform the law of corporate criminal liability, which can be done specifically to AI systems and their implementation in such essential industries as healthcare. In the era of autonomous systems and digital medicine, the criminal law can satisfy their deterring role only with such reforms.

5. Conclusion:

In healthcare, the rising popularity of Artificial Intelligence (AI) is, no doubt, a step to a new level of clinical and operational performance due to the influx of clinical accuracy, efficiency, and operational management. Nonetheless, it also has created new cybersecurity vulnerabilities, which the current jurisprudence is unprepared to use efficiently and effectively, especially when such failures result in mass damages or data theft. The paper investigated the real-life cases, legal principles, and interjurisdictional strategies to investigate the feasibility and restrictions of the imposition of corporate criminal liability in relation to an AI-induced cybersecurity breach. The analysis also shows a persistent disjunction between the application of technology and legal responsibility, mainly because of the impossibility of assigning a relevance to intent, the black box nature of AI systems, and the division of responsibility between corporate agents and those developers outside the company. Although significant breaches of security and system disruption occurred in a number of high-profile healthcare cases, no corporate criminal liability has been proved up to date, which reflects a grave enforcement gap and doctrinal gap. This absence of criminal responsibility does not only undermine the deterrent effect but also does not indicate the seriousness of the harm inflicted on patients to whose lives and privacy patients are exposed. Thus, it is the time to reconsider the current corporate liability principles and adjust them to the realities of the AI-based decision-making. The legal reforms should aim at redefining the aspects of organizational mens rea and enhancing the duty of care and incorporating accountability mechanisms in the life cycle of AI development and deployment. In highly important industries such as healthcare, where both human lives and confidential information may be at stake, this reform is necessary to preserve justice, promote resilient governance and develop the confidence of people in the technological future of medicine.

References:

- Balkin, J. M. (2017). *The three laws of robotics in the age of big data*. Ohio State Law Journal, 78(5), 1217–1234.

- Bailleux, J., & Deffains, B. (2020). *Artificial intelligence and legal responsibility: Revisiting the decision-making process*. European Journal of Law and Economics, 50(3), 381–403. https://doi.org/10.1007/s10657-020-09644-4
- Bertolini, A. (2013). *Robots as products: The case for a realistic analysis of robotic applications and liability rules*. Law, Innovation and Technology, 5(2), 214–233. https://doi.org/10.5235/17579961.5.2.214
- Calo, R. (2018). *Artificial intelligence policy: A primer and roadmap*. UC Davis Law Review, 51(2), 399–435.
- Edwards, L., & Veale, M. (2017). *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. Duke Law & Technology Review, 16(1), 18–84. https://doi.org/10.31228/osf.io/8dxv6
- Khanna, V. S. (1996). *Corporate criminal liability: What purpose does it serve?* Harvard Law Review, 109(7), 1477–1534. https://doi.org/10.2307/1342241
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). *Cybersecurity and healthcare: How safe are we?* BMJ, 358, j3179. https://doi.org/10.1136/bmj.j3179
- Meszaros, J. (2020). *Cybersecurity threats and medical AI: Challenges in legal responsibility and ethical design*. Computer Law & Security Review, 36, 105377. https://doi.org/10.1016/j.clsr.2020.105377
- Pagallo, U. (2013). *The laws of robots: Crimes, contracts, and torts*. Springer.
- Yeung, K. (2017). *'Hypernudge': Big data as a mode of regulation by design*. Information, Communication & Society, 20(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713
- Casey, A. J., & Niblett, A. (2020). *Self-driving laws*. University of Toronto Law Journal, 70(1), 24–60. https://doi.org/10.3138/utlj.2018-0040
- Calo, R., & Kerr, I. (2013). *Robots and privacy*. In Lin, P., Abney, K., & Bekey, G. A. (Eds.), *Robot ethics: The ethical and social implications of robotics* (pp. 187–202). MIT Press.
- Donovan, J., & Klugman, C. (2020). *Liability for artificial intelligence decision-making in healthcare*. Medical Law International, 20(1), 57–75. https://doi.org/10.1177/0968533220918034
- Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). *Adversarial attacks on medical machine learning*. Science, 363(6433), 1287–1289. https://doi.org/10.1126/science.aaw4399
- Hanna, J. (2019). *Corporate criminal liability in the age of artificial intelligence*. Georgetown Law Technology Review, 3(2), 472–486.
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). *Cybersecurity in healthcare: A systematic review of modern threats and trends*. Technology and Health Care, 25(1), 1–10. https://doi.org/10.3233/THC-161263
- Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). *Accountable algorithms*. University of Pennsylvania Law Review, 165(3), 633–705.
- Price II, W. N., Cohen, I. G., & Shachar, C. (2019). *Health data, technology, and the law*. Journal of Law, Medicine & Ethics, 47(2), 126–129. https://doi.org/10.1177/1073110519857326
- Singh, M., Mathiassen, L., & Mishra, A. (2020). *Organizational preparedness for AI: A healthcare case study*. Journal of Business Research, 123, 474–485. https://doi.org/10.1016/j.jbusres.2020.09.004

- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005
- Zhou, L., Parmanto, B., & Rehg, J. M. (2019). *The security and privacy implications of smart health systems*. IEEE Security & Privacy, 17(4), 64–71. https://doi.org/10.1109/MSEC.2019.2918777