İSTANBUL UNIVERSITY PRESS

Ceza Hukuku ve Kriminoloji Dergisi
Journal of Penal Law and Criminology,
JPLC 2026, 14 (1): 56–79

https://doi.org/10.26650/JPLC2026-1711852
Submitted 13.06.2025
Revision Requested 24.11.2025
Last Revision Received 19.03.2026
Accepted 27.03.2026
Published Online 12.05.2026

Ceza Hukuku ve Kriminoloji Dergisi
Journal of Penal Law and Criminology

Research Article

Open Access

The Criminal Liability of Hinotori: The Japanese Surgical Robotic Doctor

Esra Nur Bal [1] & Mohammad Abualrob [2]

[1] Uskudar University, Institute of Addiction and Forensic Sciences, İstanbul, Türkiye
[2] Lusail University, College of Law, Doha-Qatar

Abstract The rapid development of artificial intelligence (AI) and the medical robot industry offers transformative opportunities to enhance healthcare quality. Approved for production and marketing in August 2020, the Hinotori Surgical Robotic Doctor, designed for laparoscopic surgery, has become a prominent tool in robot-assisted procedures. However, the integration of robots into surgical practices introduces the risk of patient harm, raising critical questions about criminal liability. Unlike general discussions on AI responsibility, this study specifically focuses on the criminal liability of the Hinotori Surgical Robotic Doctor within the framework of causality principles and intent, eventual intent, negligence, conscious negligence, and absence of fault by evaluating the legal status and responsibility of the involved actors. The study first examines whether Hinotori Surgical Robotic Doctor can be granted legal personality. If not, criminal liability must be attributed to other actors under general criminal law principles. Subsequent sections explore the responsibilities of the software programmer, manufacturer, and healthcare providers (surgeons and hospitals). This study contributes to the literature by presenting a multi-dimensional legal analysis, offering recommendations for future legislation, and addressing a significant gap by focusing directly on the Hinotori Surgical Robotic Doctor's liability, rather than AI in general.

Keywords artificial intelligence · Hinotori · robotic surgery · criminal liability · negligence · intent · causality

Citation: Bal, E. N. & Abualrob, M. (2026). The Criminal Liability of Hinotori: The Japanese Surgical Robotic Doctor. *Ceza Hukuku ve Kriminoloji Dergisi–Journal of Penal Law and Criminology*, 14(1), 56-79. https://doi.org/10.26650/JPLC2026-1711852

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License.

2026. Bal, E. N. & Abualrob, M.

Corresponding author: Esra Nur Bal esranur.bal@st.uskudar.edu.tr

Introduction

Digital technologies are advancing rapidly in each field, and the overall immeasurable digital transformation process in front of humanity is making great progress every single day. The development of artificial intelligence and the medical robot industry are creating a new trend in this transformation, and it offers great opportunities for progress and improving the quality of life (Vuletic and Petrasevic, 2020, 226; Kitatsuji et al, 2022, 9). The Hinotori Surgical Robot System produced by the medical robot company named Medicaroid Corporation for laparoscopic surgery was approved for production and marketing, making it the device of choice for robot-assisted surgery in August 2020. In December 2020, the system was used in the first surgery, a radical prostatectomy, at the International Cancer Medical and Research Center, Kobe University Hospital, which was successfully completed (Kitatsuji, 2023, 21). Hinotori, developed to reproduce the precise movement of the surgeon necessary for surgeries, has three units: Surgeon Cockpit, Operation Unit, and Vision Unit.

Through the Surgeon Cockpit, the surgeon operates robotic instruments and an endoscopic camera while simultaneously observing the operative field through high-resolution 3D imaging. The Operation Unit translates the surgeon's commands into precise mechanical movements executed by the robotic arms during the surgical procedure, whereas the Vision Unit integrates visual data and supports coordinated communication among members of the surgical team. Although the Hinotori system incorporates advanced robotic technologies designed to enhance surgical precision and control, it does not function autonomously. Instead, the system operates as a technologically mediated platform through which surgeons remotely manipulate surgical instruments while maintaining continuous procedural control. The technical architecture of the Hinotori system is designed to enhance surgical precision while simultaneously minimizing physical interference between robotic arms and assisting personnel during operative procedures. Its compact structural configuration and articulated robotic arm system provide an expanded range of motion compared with conventional surgical instruments, thereby facilitating the execution of delicate and complex surgical interventions (Kitatsuji et al., 2022, 9–12; Kuromatsu et al., 2024, 57). In order to ensure the reliability and safety of these complex robotic operations, extensive computational simulations have been conducted to optimize the system's control algorithms. It is reported that approximately 18 trillion computerized simulation sessions were performed during the development process (Kawasaki Heavy Industries, 2021). The technology with which the Hinotori system is equipped has the potential to expand access to advanced surgical care worldwide, reduce inequalities in healthcare delivery, and contribute to surgical education through remote and distance-supported procedures (Ide, 2024, 230-238).

At the first applications, Hinotori has been used in urology. Currently, its use has been extended to the following areas: adrenalectomy, radical nephrectomy, radical prostatectomy (Motoyama et al., 2023), gastrectomy (Ebihara et al., 2023), gynecology (Suzuki et al., 2023), colon cancer (Miyo et al., 2023), pancreaticectomy (Tomihara et al., 2024), pyeloplasty (Tobe et al., 2024), rectal cancer (Katsuno et al., 2024), and sacrocolpopexy (Ichino et al., 2024).

The incorporation of robots into surgery introduces a risk in the form of the potential for harm caused for the patient by the robot independent of the surgeon's actions. Between January 2000 and December 2013, 144 deaths, 1391 patient injuries, and 8061 device malfunctions related to robotic systems and instruments used in minimally invasive surgery were reported in the FDA's MAUDE database (Holder et al., 2016, 388-390; Alemzadeh, Raman, and Leveson, 2016). These numbers reflect a fluctuating success vs. failure rate, which highlights the certain level of damage incurred by patients nationwide.

The determination of criminal liability is based on the attribution of the act to a human agent, the existence of culpability, and the establishment of a legally relevant causal link between the conduct and the resulting outcome. This structure is closely connected to the offender's capacity for free will, the ability to direct behavior in accordance with normative standards, and the capacity to foresee the unlawful result (Louis et al., 2021, 1-9; Simester, 2021, 77). Classical criminal law doctrine has largely constructed the material and mental elements of crime upon a human-centered conception of action, while technical instruments have generally been regarded as passive means in the hands of the offender (Robinson, 1993, 858). However, the increasing prevalence of artificial intelligence–assisted systems, particularly robotic platforms used in surgical interventions, has given rise to a new legal landscape that challenges these established assumptions.

Robotic surgical systems are no longer merely mechanical instruments that directly replicate the surgeon's physical movements. Rather, they are structures that actively mediate the surgical process through software algorithms, sensors, data-processing mechanisms, and automated control systems. This development gives rise to significant debates within criminal law regarding the execution of the act, the determination of fault, and the establishment of causation between the act and the resulting harm (De Micco et al., 2024, 3).

Intent (dolus) is commonly defined in criminal law doctrine as the situation in which the offender knows and wills the occurrence of a particular result as a consequence of their conduct (Parsons, 2000, 5). Accordingly, for intent to be established, the offender must know of all constituent elements of the offence, including the act, the result, and the causal link between them. Within the general criminal law doctrine, culpability is the constitutive element that establishes the moral and legal connection between the conduct and the resulting harm and as the fundamental criterion that legitimizes criminal punishment. Under this approach, criminal liability is not based merely on the occurrence of an objective harm or risk but rather on the offender's mental orientation toward the act and the normative assessability of their conduct (Robinson, 1993, 861; Taymur, 2024, 361).

The prevailing view in legal scholarship holds that the distinguishing feature between direct intent and eventual intent lies in the degree of foresight attributed to the offender. In cases of direct intent, the offender is deemed to foresee the realization of the typified result with a level of certainty approaching inevitability, whereas in cases of eventual intent, the offender merely considers the realization of the result to be possible or probable (Boğa, 2024, 128).

Criminal statutes have traditionally treated negligent offences as less serious violations than intentional ones, prescribing lower penalties accordingly. However, this penal policy has been criticized on the grounds that it underestimates the objective and subjective dangers posed by negligent conduct in modern societies. It has been argued that negligent offenders may, in certain contexts, pose a threat to society comparable to that posed by intentional offenders. For negligence to be established, the conduct must first have been carried out without intent, and the offender must have breached a duty of care aimed at preventing harmful outcomes. In addition, the offender must be blameworthy for this breach, meaning that the harmful result must have been foreseeable and preventable from the offender's perspective. Although the assessment of foreseeability necessarily involves an a posteriori evaluation, it must always be anchored in the circumstances existing at the moment the offender engaged in the criminal conduct, requiring the causal development of the act to be reconstructed retrospectively (Hakeri, 2015, 254).

In contrast to simple negligence, conscious negligence, which emerged conceptually at a later stage and occurs less frequently in practice, is characterized by the fact that the harmful result, although not desired by the offender, was foreseen. In other words, at the time of acting, the offender mentally anticipated

the specific harmful outcome that could result from their conduct. In this respect, as in cases of eventual intent, the offender is aware of the possibility that the result may occur. The decisive distinction lies in the offender's internal attitude: while in eventual intent, the offender accepts or consciously takes the risk of the result occurring, in conscious negligence, the offender acts under the belief, shaped by the surrounding circumstances, that the result will certainly not materialize (Mantovani, 2008, 365).

Strict liability constitutes a significant exception to the general principle of criminal law that an offence requires both a prohibited act (actus reus) and a culpable mental state (mens rea). Under strict liability regimes, conviction may be imposed upon proof of certain elements of the offence even in the absence of intent, recklessness, or negligence. Although strict liability is justified in practice by considerations such as procedural efficiency, the protection of public welfare, the mitigation of evidentiary difficulties, alignment of judgments with provable facts, and deterrence in high-risk activities, its compatibility with the principles of just punishment and the foundational tenets of general criminal law remains the subject of sustained doctrinal debate (Wasserstrom, 1960, 732–733; Lewna, 2023, 205–206).

Within the framework of existing positive law assessments and comparative criminal law approaches, the question of whether AI possesses a legal personality remains subject to debate. At the same time, software developers, manufacturers, surgeons, and healthcare institutions possess varying degrees of capacity to create risk, control such risk, and prevent harm throughout the process extending from the design of the system to its practical use. From the perspective of criminal law, the decisive issue lies, in connection with the debate on the legal personality of AI, in determining at which stage these actors have breached their legal obligations and how a normative link can be established between their conduct and the resulting outcome (Pagallo, 2011, 349; Bal and Sarıbey, 2025, 5-6).

It is on this legal basis that the methodological approach of the study is shaped. The study adopts a doctrinal legal research method and reinterprets the concepts of perpetration, participation, omission, culpability, and causation within the framework of AI-assisted surgical systems. The criminal liability of the Hinotori surgical robot is examined in this study on the basis of general criminal law doctrine, without being confined to any specific national legal system. The analysis is grounded in the core concepts of the general theory of crime, including act, culpability, causation, and objective attribution, with distinctions between intent, eventual intent, and negligence assessed within this framework. Rather than offering a narrow interpretation of positive law or an analysis limited to a single jurisdiction, this study evaluates the criminal liability issues arising from AI-assisted medical robots in light of established, trans-systemic principles of criminal law. Accordingly, the expression "the foundations of Hinotori's criminal liability" does not imply that the robot itself bears independent criminal responsibility, but refers, to the general criminal law criteria through which liability may be attributed to human actors involved in its design, production, and operation.

In this context, after identifying the limitations of classical theories of causation, the study introduces algorithmic-mediated causation (AMC) as a legal model designed to explain the relationship between causation and attribution in situations where algorithmic systems actively mediate the execution of the act. Rather than treating algorithms as passive instruments, AMC conceptualizes algorithmic processes as structurally relevant components of the causal chain. The model provides a normative framework for determining at which stage of the system lifecycle and to which actor criminal responsibility should be attributed when harmful outcomes emerge from the interaction between human conduct and algorithmic decision-making. In doing so, the study exposes doctrinal blind spots within existing causation theories and offers a systematic theoretical foundation capable of informing future legislative and doctrinal developments.

Beyond its theoretical contribution, the study is original in scope, as there is currently no academic work that directly examines the criminal liability implications of the Hinotori surgical robot. By focusing on Hinotori as a concrete and high-risk application of AI-assisted surgery, the article demonstrates that prevailing criminal law approaches—largely structured around a perpetrator–instrument dichotomy—are insufficient to capture the normative complexity introduced by algorithmic mediation. Therefore, the article's contribution lies not only in addressing an unexamined case but also in showing how algorithmic mediation fundamentally reshapes both the execution of the act and the structure of causation, thereby challenging the adequacy of traditional human-centered liability frameworks in criminal law.

I. Methodology

This study employs a qualitative legal research methodology aimed at systematically investigating the potential criminal liability associated with the Hinotori Surgical Robotic Doctor. The research is grounded in a doctrinal analysis approach, entailing an in-depth examination of established legal doctrines, statutory frameworks, and scholarly discourse pertinent to AI, robotics, and criminal law. Doctrinal legal research constitutes the primary methodological framework of this study. The analysis is grounded in a systematic examination of the general criminal law doctrine.

In addition, secondary sources have been consulted, including international legislative frameworks related to AI, as well as case reports and regulatory documents issued by the United States Food and Drug Administration concerning medical devices and AI-assisted systems. These secondary materials are employed to contextualize the legal analysis within its technical and regulatory environment.

The research design integrates a comprehensive review of existing literature on robotic-assisted surgical technologies, with a particular focus on the Hinotori system's technical specifications, operational mechanisms, and regulatory context. The legal evaluation is structured around four primary categories of actors potentially subject to liability: (1) the robotic system itself, (2) software developers, (3) manufacturing entities, and (4) healthcare practitioners and institutions, including surgeons and hospitals. The responsibilities and possible legal ramifications for each actor are assessed through the analytical framework of general criminal law principles.

To critically engage with questions of causality, the study adopts and applies three central theoretical models: the theory of equality of circumstances, the theory of plausible cause, and the theory of efficient cause. These models facilitate a nuanced assessment of how liability may be distributed depending on the presence or absence of subjective fault elements, such as intent or negligence. Building on the limitations identified within these traditional approaches—particularly in the context of algorithmically mediated conduct—the study further proposes a novel causation framework, the algorithmically mediated causation (AMC) model, specifically designed to address the unique causal architecture of offences arising from AI-based and robot-assisted systems. In addition, the study addresses the practical challenges posed by the absence of AI-specific legislative frameworks and offers an evaluative exploration of potential pathways for future regulatory and normative development.

II. Criminal Liability of Hinotori

In addressing the current landscape of AI regulation, it is essential to recognize that no harmonized global framework exists yet to explicitly govern the criminal liability of AI systems. Nevertheless, several jurisdictions have begun to grapple with this issue indirectly through emergent regulatory schemes. The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the

Council of June 13, 2024 laying down harmonized rules on artificial intelligence) predominantly emphasizes safety, transparency, and risk governance, deliberately deferring questions of criminal accountability to the discretion of national legal systems. In the United States, although no federal statute specifically addresses the criminal liability of AI, sector-specific regulations — such as the FDA's oversight of medical devices — impose binding obligations on manufacturers and developers, under which criminal sanctions may arise in instances of gross negligence or willful misconduct. China's regulatory model, by contrast, centers on algorithmic transparency and stringent state oversight, emphasizing administrative and civil sanctions, while substantive debates on criminal liability remain at an incipient stage. Japan, as the jurisdiction of origin for the Hinotori system, continues to adhere to general criminal law principles, attributing liability exclusively to human actors and refraining from extending independent legal personality to AI entities. Across these legal landscapes, a common challenge endures: the adaptation of conventional criminal law paradigms to the novel complexities and diffuse accountability structures introduced by AI-based technologies (Kan, 2024, 146; Köken, 2021, 251; Kuklińska, 2021, 2; Abdelaziz, 2025, 2).

The criminal liability of the Hinotori surgical robot system must be examined from a multidimensional perspective. As an AI-assisted system, Hinotori's legal status and the roles of different actors should be analyzed separately. Therefore, structuring this section of the article around Hinotori's legal status, followed by the roles of the software programmer, manufacturer, and healthcare providers (surgeons and hospitals) allows for a comprehensive and systematic analysis of the liability chain.

A. The Issue of the Legal Personality of Hinotori and Human Interaction

In order to solve the criminal liability that Hinotori will create, its legal status/personality must first be determined. The most important factor in terms of criminal liability is free will. Presently, AI can perceive the outside world through machine learning and deep learning and can generate solutions for similar or different problems with less effort and more productivity than humans. Nevertheless, AI is not self-aware or conscious of its past (Köken, 2021, 262; Kan, 2024, 284).

A comparative analysis of existing regulatory instruments across major legal systems reveals a clear and consistent doctrinal stance: AI is not recognized as a legal person under any current positive law, nor is it attributed autonomous legal standing or capacity (Ziemianin, 2021; Filipova and Koroteev, 2023; Pinkevich and Konev, 2024, 89). The most comprehensive and binding regulatory instrument to date, the European Union Artificial Intelligence Act (EU AI Act, 2024), explicitly defines AI in Article 3(1) as *"a machine-based system that is designed to operate with varying levels of autonomy... and that infers from input how to generate outputs such as predictions, content, recommendations, or decisions."* This definitional choice is of critical importance, as it places AI within the category of *technologically engineered systems*, rather than legal subjects capable of bearing rights or obligations. Subsequent provisions of the Act assign legal accountability exclusively to human "providers," "deployers," and "users," thereby normatively excluding the possibility of AI possessing legal personhood.

This regulatory position is not unique to the European Union but is mirrored across other major jurisdictions. In the United States, neither the Blueprint for an AI Bill of Rights (2022) nor the Executive Order on Safe, Secure, and Trustworthy AI (2023) confer any form of legal subjectivity upon AI; instead, AI is defined as a machine-based decision-support system, while legal and ethical responsibility is anchored in human actors. Similarly, China's Regulations on the Administration of Generative Artificial Intelligence Services (2023) and Russia's National Strategy for the Development of Artificial Intelligence (2020) conceptualize AI as a technological tool embedded within human-controlled socioeconomic systems without affording it a juridical agency. From the standpoint of international law, no treaty or customary norm recognizes AI as a subject of international legal personality, a status reserved strictly for states and international organizations.

Accordingly, it can be conclusively stated that AI within all existing legal frameworks—including the EU AI Act (2024), the U.S. Executive Order on AI (2023) and AI Bill of Rights (2022), China's Generative AI Regulation (2023), and Russia's AI Strategy (2020)—is not attributed to legal personality.

Therefore, for now, the Hinotori Surgical Robot System must be characterized as a type of tool (Rivero-Moreno, Echevarria, and Vidal-Valderrama, 2023), perhaps an object, device, or weapon in the context of criminal law until it is given any other status. From the standpoint of criminal jurisprudence, the characterization of AI not as a juridical perpetrator but as an instrument of human agency constitutes not merely a doctrinal preference but a categorical consequence of the ontological architecture of legal responsibility. Criminal liability is predicated on the existence of a norm-responsive agent capable of volitional orientation, moral cognition, and susceptibility to censure—attributes conceptually inseparable from personhood. AI systems, despite their capacity for autonomous operation and adaptive decision-making, function as computational mechanisms devoid of men rea, normative intentionality, and the phenomenology of will. They do not interpret legal norms as reasons for action but merely execute algorithmic outputs in accordance with preconfigured parameters. Accordingly, AI cannot be situated within the class of entities capable of bearing criminal responsibility; rather, it operates as an extension, amplification, or instrumentality of human decision-making power. Within this normative framework, AI is not a locus of culpability but a technologically mediated vector through which human agency is externalized, thereby necessitating that liability be ascribed exclusively to the natural or legal persons who exercise control over its design, deployment, or operation (Köken, 2021, 262; Kan, 2024, 289).

Thus, the mens rea, which includes the intention or knowledge of wrongdoing that constitutes a part of the offence, and the actus reus, which is expressed as the criminal act in addition to the perpetrator or indirect perpetrator, will be evaluated within the framework of other potential actors such as software programmer, manufacturer, and healthcare providers.

B. Software Programmer

Robotic surgical systems, including Hinotori, have software programed to allow surgeons to operate with high precision in tight spaces or very small tissues, using data provided by artificial intelligence to perform more accurate and precise movements when operating. The surgical robot Hinotori has certain important features arising from the software that differentiate it from existing systems, including: software calibration of the trocar position without the need to attach the trocar (Ide, 2024, 235). Furthermore, the pivot position is maintained through software control to eliminate the mechanism of holding a tubular device called a trocar cuff, which is inserted into the patient's abdominal wall (Kitatsuji et al., 2022, 10).

The ability of the Hinotori surgical robot to calibrate the trocar position automatically through software, without the need for manual adjustment, and maintain the pivot point via software control without reliance on a mechanical apparatus introduces a form of technical autonomy that attenuates the direct human dominion over the act in question from the perspective of criminal law. This functional architecture raises a fundamental inquiry whether the surgeon retains conscious control and normative authority over the material element (actus reus) of the surgical act at all stages of its execution. The software-based features of Hinotori create the impression that, in certain decisive stages of the intervention, the act is not executed solely through human volition but is partially mediated by algorithmic control mechanisms. Consequently, the normative assessment of objective attribution becomes increasingly complex, as it must determine whether the legally relevant risk was generated by the surgeon, the software system, or the designer, manufacturer, or other institutional actors involved in configuring the system. Accordingly, Hinotori's software-controlled calibration and pivot stabilization are not merely technical innovations; they constitute

a transformative legal parameter that reconfigures the identity of the perpetrator, the determination of culpability, and the normative locus of criminal responsibility.

Certain risks and faults arising from the software of Hinotori can have various consequences. If the operational software erroneously generates uncontrolled actions, it could cause injuries to the same organs and surrounding blood vessels. The faults as follows: communication connection points, creation of the operation plan, integration of audio-visual data, cyber attacks, receiving errors of unknown cause in units, system stopping, not responding, loss of axis control of arms, or acting on its own during the surgical operation are caused by software. Lack of updates for the robotic operating system, firmware, and software can cause various cyber attacks. The surgical robot, whose key advantage is remote access, could be vulnerable to faulty and malicious access, especially if unsecured and open wireless and communication ports, as well as unused ports are not programed to be securely closed (Yaacoub et al., 2022, 123). In such cases, injuries, deaths, and occasional machine malfunctions may occur, as well as the occurrence of these risks and errors may cause the surgical operation to be prolonged and the patient to remain under anesthesia for a longer period.

The behaviors that constitute the focal point of criminal law must have certain characteristics to qualify as an action. In this respect, the most important issue for criminal liability is voluntary (free) will (Köken, 2021, 269). For Hinotori, whose field of activity is programed by human hands, voluntary (free) action is out of the question for the time being. This act, on which the offence committed by Hinotori depends, may have arisen as a result of intent or negligence. If the offence is committed as a result of the programming of Hinotori by the software programmer to injure or kill the patient during the operation, then the software programmer will be held liable intentionally as a direct actor in the crime. If the Hinotori, which is programed to commit a crime, is also deliberately produced for this purpose and consciously used by hospitals or surgeons, it can be stated that the software programmer, the manufacturer, and the healthcare providers have participant control over the commission of the crime. Each accomplice is in the position of the actor. In determining whether joint dominance over the offence has been established, the roles and contributions of the co-perpetrators in the performance of the offence and the importance of their contributions should be considered. Each joint perpetrator must make an effective and functional contribution to the execution of the offence. Furthermore, if the offence committed by Hinotori is more serious than the offence expected by the software programmer or if it is another offence, criminal liability will be determined in accordance with the provisions on aggravated offences.

Indirect perpetrator is the commission of an offence by using another person as an instrument. The person in the background exercises complete control over the person who performs the executive acts of the offence. Indirect perpetrator will be the case when the person committing the offence is used as a vehicle (Köken, 2021, 273). Hinotori does not have a "legal personality" and is defined in the context of Criminal Law as an instrument, which includes among other things a "tool, device, object or weapon" and not as the person who had committed the offence. There can be no indirect perpetrator, and the software programmer will be liable as the direct actor. In order for liability as an instigator to arise, Hinotori must have a legal personality just as in the case of an indirect perpetrator, and the software programmer must have induced the decision to commit the offence in Hinotori. Therefore, it is currently not also possible for the software programmer to be liable as an instigator.

In the context of robotic medical systems, the software developer's duty to monitor and mitigate risks is not merely a technical design consideration but constitutes a normative sphere of responsibility grounded in the principles of attribution and culpability in criminal law. Criminal liability does not rest solely upon a material causal link; rather, it hinges on whether the individual had control over the risk domain and whether

the risk was foreseeable and preventable. The incorporation of adaptive risk management, threat modeling, AI-assisted anomaly detection, real-time monitoring, regulatory compliance mechanisms, periodic software updates, secure coding practices, and robust system architecture throughout the device's lifecycle—from design to deployment, use, and maintenance—demonstrates that the developer exercises not only technical but also legal and factual control over the system's safety profile. In such circumstances, the developer is not a mere "code engineer" but a normative agent exercising decisive influence over the creation, continuation, and elimination of risk; thus, culpability arises not simply from causal contribution but from the breach of a professional duty of care (Gordon et al., 2022, 148; Marcus et al., 2024, 62; Vulpe et al., 2021; Terwoort et al., 2020).

Conversely, where risks are only theoretically foreseeable and the developer lacks technical access, legal authority, or operational capacity to intervene within the system's lifecycle, criminal liability cannot be founded solely on causal connection, as such an approach would contravene the principle of culpability. Culpability does not stem from the mere existence of a causal link but from a violation of the normative duty incumbent upon the actor—that is, from the failure to exercise the level of care expected from a reasonable software developer in the given context. Accordingly, where early integration of security measures, dynamic risk management, continuous anomaly detection, periodic software updates, and compliance with cyber-security standards are available yet are not considered, the developer's inaction may constitute culpable omission (Giannini and Kwik, 2023, 51).

In this regard, the developer's role in the safety architecture of a robotic medical system materializes the duty of care in criminal law terms: responsibility shifts from static authorship of code to an active and ongoing obligation to ensure the integrity and security of a continuously operating technological system. Therefore, insofar as the developer possesses effective control and intervention capability—via security-by-design, continuous monitoring mechanisms, and post-market update and oversight obligations—an obligation to observe and mitigate risks arises. Failure to discharge this obligation, where it normatively contributes to harm and where a foreseeable risk remains unaddressed despite available preventive measures, may give rise to criminal liability for omission. Accordingly, in the realm of robotic medical technologies, the software developer's liability cannot be assessed solely through causal analysis but must be determined through a combined evaluation of attribution, foreseeability, intervention capacity, and culpability (Kowert, 2017, 192).

If more than one person, who together have an obligation to prevent a certain result, neglects their obligation to prevent this result together and the result occurs, the perpetrators may be held liable as the participant perpetrator (Öztürk, 2023, 273-274). Thus, attention should also be drawn to the hospitals responsible for supervision and care and to surgeons who do not report any hazards or risks. In this case, they will be held responsible as the participant perpetrator along with the software programmer.

The main problem regarding criminal liability is how to proceed in the absence of intent or negligence. In other words, the crime committed by Hinotori may not have arisen from the software programmer's intent or negligence. For instance, the software programmer may have designed the software in good faith, ensured it underwent rigorous testing, and minimized all foreseeable risks. However, the possibility remains that unforeseen algorithmic deviations and unexpected software errors could still contribute to the commission of the offense. In this case, the "connection of causality" will be discussed. According to the theory of equality of circumstances, all conditions that are effective in the occurrence of the result are of equal importance. The fact that the conditions that are foreign to the perpetrator are included in the plot does not mean that the causal connection will be interrupted. In the theory of plausible cause, for an act to be accepted as having a causal value in terms of a consequence, it must be an appropriate act for the occurrence of the

consequence. Under the efficient cause theory, only a condition that cause an outcome is the efficient cause. The others are termed occasions (Akbaba, 2021, 19-35; Reinach, 2009, 7-18).

Hinotori's software programmer is the person who has constant command over Hinotori and provides the essential service for operating the surgical robot. The key to all the capabilities of AI, the brain, the core, and its components is code (Beard et al., 2009, 30). Since Hinotori qualifies as a "tool, object, device, or weapon" in the context of Criminal Law, the "software" created by the programmer would also qualify as a tool for any offence committed by Hinotori.

Based on the theory of equality of circumstances, in the case of an offence committed by Hinotori, even if the software programmer had no intent or negligence, merely because he/she provided the instrument for the offence by creating the software, the created instrument would be equally effective as other causes in the commission of the offence. Therefore, even in the absence of intent or negligence, he or she would be criminally liable to an equal degree with other actors as a participant. According to the theory of plausible cause, the criminal liability of the software programmer is more limited than under the theory of equality of circumstances. Here, the judge will determine which of the causes of the consequence is legally significant. The software programmer will be criminally liable as an involved if the software programmer's creation of the software and the provision of an instrument is considered to be an act suitable and convenient for the commission of the offence (Doğan, 2011, 114; Centel, Zafer and Çakmut, 2005; 268).

However, in the absence of intent or negligence on the part of the software programmer, it is impossible to establish a causal connection between his/her action and the result according to the theory of plausible cause because this theory requires at minimum a reasonable probability that the actor's conduct contributed to the result in a normatively relevant way. In Hinotori, however, the programmer's mere act of creating or deploying software remains too remote, both factually and normatively, to satisfy this threshold: the harmful outcome emerges only after a chain of algorithmic processes, system-level interactions, and user-dependent decisions that the programmer cannot reasonably foresee or control. As a result, the programmer's contribution does not reach the level of "plausibility" required for attribution under this theory. Since it is not possible for him/her to know or predict the crime committed by Hinotori by merely creating the software instrument, criminal responsibility cannot be mentioned. In the efficient cause, the software created by the software programmer, i.e. the tool provided by the software programmer, is only an occasion for the realization of the result. In the absence of intent or negligence on the part of the software programmer, the software programmer will still be liable for providing the software, i.e. the tool. However, criminal liability will arise in the actual cause of the offence, and since the act of the software programmer will be considered an occasion, the criminal liability will be less than the actual act causing the result as an involver (Hafızoğulları and Özen, 2012, 204; Wright, 2014).

C. Manufacturer

The manufacturer of the Hinotori Robotic Surgery System, like manufacturers of other medical devices, has high responsibilities for safety, performance, regulatory requirements, and the health of users. This responsibility extends from the beginning of the manufacturing process to after-sales support. Firstly, the manufacturer's main obligations are the safe and effective design of Hinotori. The design must have features specifically aimed at minimizing human error, as medical interventions can entail a high risk. Secondly, while an important feature that distinguishes Hinotori from other robotic surgery systems is its ergonomics, the manufacturer must ensure that the device is comfortable and safe to use. Similarly, the manufacturer must implement rigorous and thorough testing protocols to ensure that Hinotori functions correctly (Razek, 2023, 1-20). It is also the manufacturer's responsibility to perform risk assessment processes on an ongoing basis to identify potential risks and make the necessary improvements.

The manufacturer must ensure that Hinotori is legally compliant with health and safety standards and regulators, that the necessary audits on biocompatibility, sterilization and safety have been conducted, and that the relevant certificates have been obtained. Moreover, the manufacturer must establish post-market traceability of the product even after Hinotori has been placed on the market and must record and notify the relevant health authorities of any situation requiring enhanced safety and improvements, or any adverse events occurring in the use of the robot. It should also provide continuous support for the maintenance and repair of the robot and provide training programs for surgeons and other healthcare personnel on the safe and effective use of Hinotori (Razek, 2023, 14; Börü Parlak, 2019, 763). This training should cover operational aspects as well as how to respond to possible emergencies.

The manufacturer shall be deemed to have direct intent if the manufacturer knows that the device will operate in a defective, dangerous, or criminal manner and acts willingly with this result, or if it intentionally left a defect during the production of the device and foresaw that this defect could cause a crime. If the manufacturer foresaw that the robot could potentially cause harm but decided to take the risk and release the product to the market, this constitutes eventual intent as in cases where the device is placed on the market by the manufacturer without completing safety tests or passing the relevant inspections. In both situations, if Hinotori commits an offence, the manufacturer will be held liable as the actor. If other persons intentionally acted in the occurrence of the offence, for instance, the hospital continue to use Hinotori, knowing of this fault and hazard, each of the actors will be held liable as a participant.

In cases where the manufacturer acts with simple negligence or conscious negligence, it is necessary to establish a connection between the offence committed by Hinotori and the action of the manufacturer (Pepito et al., 2019, 935-937; Boscarato, 2011, 405). According to the theory of equal circumstances, the manufacturer is liable as an actor if it did not demonstrate the necessary care and diligence during the design or production of the device and caused the offence to occur due to this negligence. For example, the manufacturer may have failed safety tests or failed to detect mechanical defects or risk assessment. In this situation, when it is accepted that the manufacturer has no intention in the realization of the offence, it can be suggested that their actions remain at the level of negligence, but in cases where the level of simple negligence is exceeded and the manufacturer can foresee but does not take the necessary precautions, it will be held responsible with a heavier penalty. Since this theory considers all contributions to the offence equal, even if there are other factors that constitute the offence, the responsibility of the manufacturer will be definite, and they will be held equally responsible with other actors (Doğan, 2011, 114; Centel, Zafer and Çakmut, 2005; 268).

According to the theory of plausible cause, the existence of a negligent act of the manufacturer is considered proximate cause only if it can be expected that this act will make it possible for the device to commit an offence, and the manufacturer is held liable as an actor. For example, if the manufacturer can foresee that the materials used in the production of Hinotori are capable of causing a malfunction in a short time, it can establish a proper cause relationship with this result, but if the device commits an offence as a result of the loss of control of the device by a cyber attack, the manufacturer's negligent behavior will not be accepted as a proper cause, and the manufacturer's liability will not arise (Hafızoğulları and Özen, 2012, 204).

The effective cause states that if the manufacturer's negligent behavior is considered the most effective cause of Hinotori's offence, the manufacturer shall be liable. However, even if the manufacturer did not fulfill its obligations and acted negligently, if the most effective cause of Hinotori's offence includes, for example, surgeon's misuse of the device or the hospital's failure to ensure regular maintenance of the device, the manufacturer's contribution is not considered an efficient cause. In this case, the manufacturer's liability

may be diminished or eliminated. It is necessary to look at the direct contribution of the manufacturer's negligent act to the result and its degree (Wright, 2014; Dönmezer, 2003, 140).

In the absence of intent or negligence on the part of the manufacturer, criminal liability may be considered in terms of certain factors. For example, if Hinotori contains a high-risk technology that poses a risk to public or individual health and a potential danger to public or personal safety and public order, the criminal liability of the manufacturer, who has the broadest powers over the product, may arise. However, this matter will likewise necessitate distinct and comprehensive treatment within the framework of compensation law. Administrative and regulatory sanctions such as license revocation or fines, may also be imposed on the manufacturer.

D. Surgeons and hospitals

The surgeons should act based on both medical and technological knowledge when using robotic systems such as Hinotori. The obligations of surgeons are as follows: completion of robotic surgery training and continuous learning under the heading of education and expertise obligation; correct use and anticipation of risks under the heading of device use obligation; planning the necessity of robotic surgery and risk information under the heading of patient safety; control during the operation and preparedness for emergencies under the heading of continuous observation and intervention; and finally reporting malfunctions, errors, and risks (Matsuo, 2018, 87-102; Walden et al., 2017, 3034).

The hospital should pay attention to reliability, certification, and suitability criteria when choosing a robotic surgery system. It should ensure regular maintenance of Hinotori and perform the necessary software updates and system controls. In addition, it should provide surgeons with robotic surgery training and regularly test whether surgeons have sufficient knowledge and skills in this regard. It is the responsibility of both the surgeon and the hospital to check whether Hinotori is working before each operation. Hospitals should also develop manual intervention methods in any case where Hinotori fails, and problems related to the robot should be regularly monitored, identified, and reported. Quality control systems should be established to guarantee the safe and effective operation of the robotic surgical system. Informing and obtaining the consent of the patient, protecting the data obtained from Hinotori, and patient confidentiality are the responsibility of the hospital as well as the surgeons (Rathnayake, 2024, 31; Walden et al., 2017, 30-34).

If surgeons or hospitals intentionally breach these obligations and their intentional actions cause the offence, they will be liable as an actor or, if they act in concert with other actors, as a participant. If the surgeon or the hospital foresaw that the device could commit an offence but continued to use it by taking this risk, eventual intent will be in question. For example, if the surgeon or hospital knew that the device had a clear defect but continued to use it, eventual intent is in question. In this situation, criminal liability will be less than direct intent. In comparative criminal law, eventual intent (dolus eventualis) is generally regarded as a form of culpability that reflects a lesser degree of blameworthiness than direct intent (dolus directus). Most criminal justice systems distinguish direct intent, eventual intent, and negligence, and the severity of punishment typically escalates according to the actor's mental state. Because eventual intent embodies a less immediate volitional commitment to the prohibited result—where the actor foresees the possibility of the harmful outcome yet proceeds nonetheless—it is commonly associated with sanctions less severe than those imposed for direct intent but more serious than those applied to negligent conduct. This gradation is grounded in foundational principles such as proportionality, which demand that the intensity of punishment corresponds to the seriousness of the offender's mental attitude and the harm produced (Husak, 2022, 172). However, there is a significant body of opposing doctrinal opinion. According to this view, eventual intent remains a manifestation of intent and should therefore be punished in the same manner as dolus directus. No theoretical framework, these scholars argue, justifies a reduction in penalty on the basis

of conditional intent; on the contrary, prevailing theories support the imposition of identical sanctions, emphasizing that foreseeability and acceptance of the prohibited result constitute a sufficient volitional foundation for full intentional liability (Gökpınar, 2008, 222).

In the context of robot-assisted surgical systems, such as Hinotori, harmful outcomes may indeed be linked to the conduct of surgeons or hospitals; however, the dogmatic structure of criminal responsibility requires distinguishing omission from negligence, concepts that are often blurred in practice. The mere fact that a surgeon "failed to take precautions" or that a hospital "failed to maintain the device" does not immediately indicate negligent behavior; rather, these circumstances must first be examined as violations of a legally relevant duty to act (omissive conduct). Only after establishing a duty existed and was breached can the analysis shift to the degree of fault that accompanies the omission.

For example, if a surgeon receives a navigation-error alert from the Hinotori interface but does not initiate the required verification protocol, the core issue is not yet whether the surgeon acted negligently but whether they failed to perform an act that the law and the professional standard objectively required —namely, the duty to respond to a critical system warning and the duty to intervene in clinically significant blood loss. Similarly, if the hospital allowed the device to be used without timely maintenance or failed to provide adequate training to the surgical team, these circumstances primarily constitute institutional omissions arising from legally recognized obligations to ensure the safe operational condition of the device and the competence of its users.

Once such omissions are established, the next step concerns the mental state accompanying the failure. If the surgeon or hospital simply overlooked a risk, misinterpreted a system alert, or mistakenly assumed the device to be functioning properly, their liability would fall under simple negligence. Conversely, if they were aware of the relevant risk—such as recurrent calibration errors, overdue maintenance logs, or insufficient operator competence—yet deliberately chose not to intervene, the conduct constitutes conscious negligence, a more aggravated form of fault that is typically sanctioned more severely than simple negligence. This is because the actor's actual foresight of the risk and volitional decision to proceed regardless places their blameworthiness closer to the domain of intent, thereby justifying a correspondingly harsher penal response (Loveless, Allen & Derry, 2020, 130).

Accordingly, although surgeons or hospitals may be held responsible where a causal connection between their failure to act and the harmful outcome can be established, the severity of punishment must reflect the doctrinal distinction between omission and negligence: the former identifies what duty was breached, whereas the latter evaluates the degree of blameworthiness with which the breach occurred. The failure to maintain this analytical separation risks conflating fundamentally different forms of wrongdoing and obscuring the multi-layered responsibility structure inherent in Hinotori.

In the event that they act negligently or intentionally, the responsibility for the surgeons and the hospital within the framework of the causation theories will be established as follows: according to the equal circumstances theory, the actions of each actor will be considered equally necessary in the occurrence of the result and they will be punished equally. In the theory of plausible causation, whether acting with intent or negligence, if the party's action is not conducive to the commission of the offense, liability may be reduced or eliminated if the conducive factor is a different factor (Doğan, 2011, 214; Hafızoğulları and Özen, 2012, 204).

In the efficient cause theory, for the criminal responsibility of the hospital or surgeon to arise, their negligent or intentional behavior must be the efficient cause of the occurrence of the crime. If the surgeon's or hospital's action is characterized as merely an occasion and not an efficient cause, liability may be less or non-existent. For example, in a case where the surgeon violated Hinotori's operating procedures, but the offence was caused by a failure in the robot's software, liability may not be attributed because the surgeon's

act was not the main cause of the offence. In contrast, if it is determined that the surgeon's negligent or intentional behavior had even an indirect effect on the occurrence of the crime, they will be held responsible, but their punishment will be more limited than that of the main cause (Wright, 2014; Dönmezer, 2003, 140).

In the absence of negligence or intentional act of the surgeons and hospitals in relation to the crime committed by Hinotori; again, an examination can be made according to the theories of strict liability and causation. Although the principle of strict liability is exceptional in Criminal Law, it can be applied in some cases. The fact that surgeons and hospitals are among the subjects that provide primary health care services, the existence of situations that pose a danger to patient safety, even if they do not have negligence or intent in some special legal regulations, can be considered sufficient for them to be responsible. If such regulations do not exist, it can be argued that in general, surgeons and hospitals will not be held liable if they fulfill their obligations and do not act intentionally in the occurrence of the offence.

However, the equal circumstances theory, which draws a stricter liability framework than other causation theories, argues that even if there is no negligence or intentional behavior of the surgeons or the hospital, criminal liability may arise if their actions can be defined as a necessary element for the realization of the crime. Even if surgeons and hospitals do not have intent, it is more likely that liability will be addressed within the scope of compensation law or in the context of administrative sanctions.

III. Discussion

The issue of the criminal liability of the Hinotori Surgical Robotic Doctor is a complex and multi-dimensional matter that must be examined within the confines of national legal frameworks and at the intersection of global legal norms, ethical principles, and technological advancements. This study establishes that, given Hinotori's lack of legal personality, it cannot be held directly liable as an offender. Accordingly, criminal responsibility must be ascribed to human actors —software programmers, manufacturing companies, surgeons, and hospitals. However, the central challenge lies not only in distributing responsibility among these actors but also in determining which causal framework should underpin liability and under what circumstances each actor may be deemed legally accountable.

Causation denotes the factual nexus linking the act to the actor, whereas attribution concerns the normative process through which the resulting conduct is legally imputed to that actor. Because no individual may be held criminally liable for an outcome to which they did not causally contribute, the resulting harm must be traceable to the person's conduct. In this respect, human behavior constitutes the "cause" element within the causal chain. Accordingly, the result prescribed in the legal definition of the offence can give rise to criminal responsibility only insofar as it emerges from a human act (Şenol, 2025, 206; Dharm et al., 2024, 53). Artificial intelligence–assisted robotic surgery systems shift the causal inquiry in criminal law beyond the traditional anthropocentric paradigm. Unlike conventional medical interventions in which the surgeon's motor actions and cognitive choices directly instantiate the actus reus, robotic platforms partially mediate this conduct through layers of software architecture, algorithmic error-correction routines, motion-stabilization protocols, and safety-governing code. Accordingly, the three classical theories of causation in criminal law require critical reassessment in this technologically hybrid context (Fernández Llorca et al., 2023, 619-620).

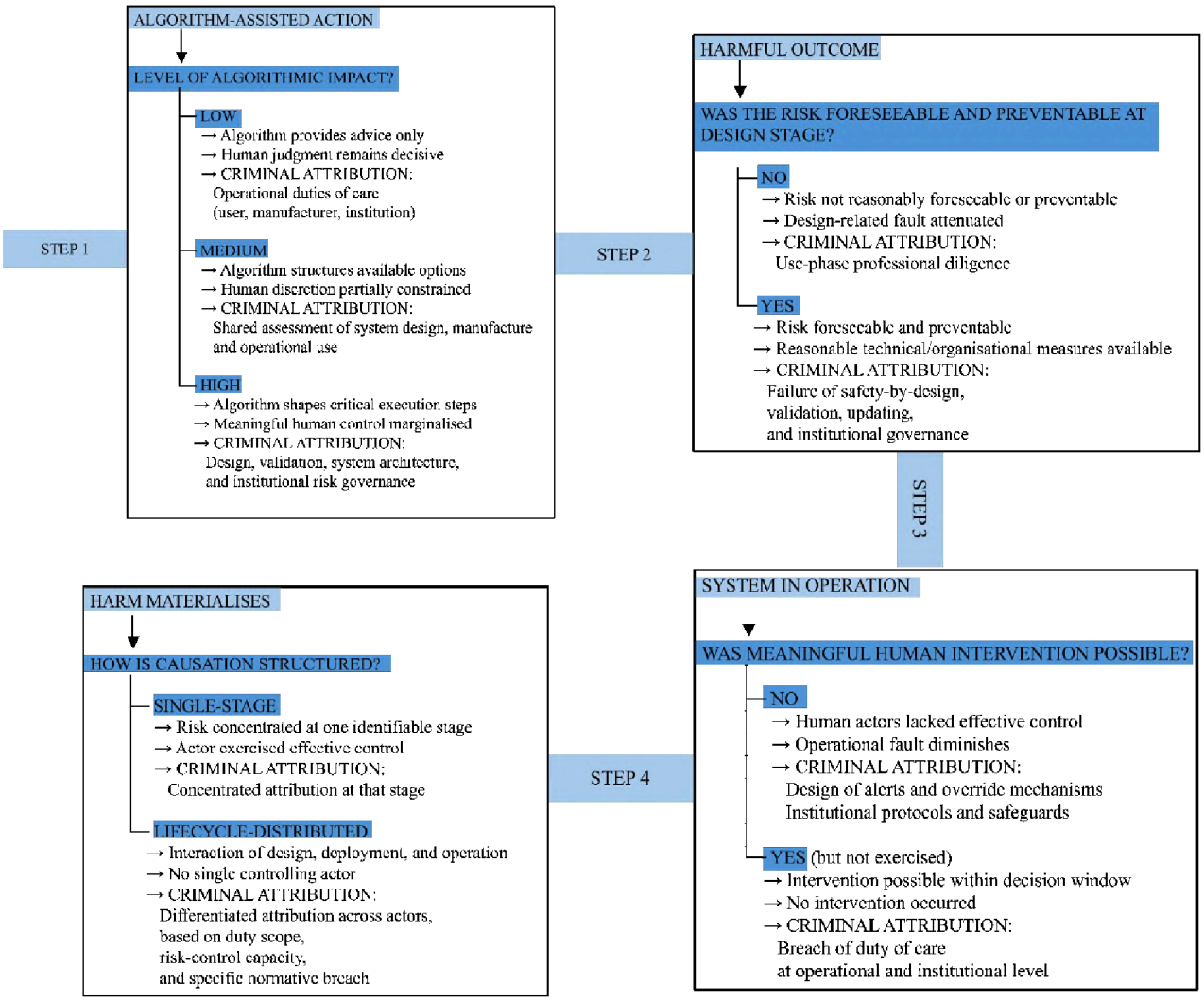
Under the equal circumstances theory, all conditions indispensable to the occurrence of the result are treated as equally constitutive causes. This generates an excessively expansive attribution framework that collapses the normative distinctions between substantially different forms of contribution. In the context of robotic surgery—where algorithmic decision-making processes, human interventions, design-level engineering choices, and institutional maintenance practices jointly shape the operative environment—this

theory would indiscriminately classify heterogeneous contributions as equivalent causes. Such overinclusiveness risks violating proportionality, undermining culpability principles, and eroding the differentiating function of criminal responsibility. The plausible causation theory narrows the causal field by requiring a sufficiently plausible link between the actor's conduct and the result. While attractive in its attempt to constrain liability, the theory becomes epistemically unstable in AI-mediated environments. Determining "plausibility" becomes problematic when algorithmic opacity, adaptive system behavior, and real-time sensor integration obscure the causal pathways between human conduct, system outputs, and harmful outcomes. Moreover, in robotic surgery, many algorithmic failures (e.g., calibration anomalies, software bugs, and silent sensor drifts) occur at levels beyond the actor's epistemic or operational control. Thus, plausible causation becomes an inadequate doctrinal instrument for capturing technologically distributed harm. The efficient cause theory, which seeks to isolate the "operative cause" of the result from mere "occasional conditions," also proves insufficient in distributed agency contexts. In robotic surgery, identifying whether the efficient cause theory is a software malfunction, a surgeon's limited ability to override system errors, or a latent maintenance defect becomes conceptually indeterminate. The cause/occasion dichotomy is structurally unsuited to multi-layered causal architectures in which algorithmic processes and human decision-making jointly constitute the actus reus. Consequently, the theory risks both over-narrowing liability and generating unwarranted exculpation. Among the three, the plausible causation theory offers a more constrained and seemingly manageable framework; however, its reliance on probabilistic and epistemic assessments makes it fundamentally incompatible with the opacity and complexity of algorithmic systems. None of the classical models adequately account for algorithmic influence, real-time autonomy gradients, or differentiated intervention capacities of human actors within technologically dense operational settings. As such, the traditional causation doctrine becomes structurally misaligned with offences arising from AI-based and robot-assisted systems (Caşın and Başkır, 2021, 43; Karnow, 1996, 181).

For these reasons, this study proposes the algorithm-mediated causation (AMC) model as a doctrinal framework tailored to AI-assisted surgical environments. The AMC constitutes a normative causation model specifically designed for acts mediated through algorithmic processes, transcending the anthropocentric and linear causal assumptions that underpin classical theories, such as the equal circumstances theory, plausible causation theory, and efficient cause theory. Rather than conceptualizing conduct through a binary schema of human act to result, AMC reconceives the operative event as a multi-layered causal architecture in which human agency, algorithmic operations, and the resulting harm are jointly and interactively produced. In this framework, the locus of causation is not limited to the immediate human action but extends to the algorithmic systems that structurally shape, constrain, or partially determine the trajectory of the actus reus. It comprises four analytical pillars. The algorithmic effect intensity principle examines the degree to which software deterministically shapes surgical output (e.g., automated trocar calibration, pivot-stabilization logic, and enforced safety thresholds). The Design-Level Preventability principle assesses whether a hazard could have been prevented through established engineering and cybersecurity protocols, including threat modeling, lifecycle security integration, and fail-safe architecture. The Run-Time Intervenability principle scrutinizes whether the surgeon or technical operator retained a meaningful, real-time ability to interrupt or override algorithmic conduct. Finally, the dual agency attribution principle determines the point at which dominant responsibility transitions from humans to algorithmic system or vice versa.

Figure 1

AMC – Four-Factor Framework for Determining Criminal Responsibility



In order to enhance the practical applicability of the AMC model, courts and prosecutors may structure their legal assessment through a series of evaluative questions. These questions clarify how responsibility should be attributed in situations where harmful outcomes arise from the interaction between human actors and algorithmically mediated systems. In particular, the following analytical inquiries may guide judicial evaluation:

1. To what extent did the algorithmic system materially influence the execution of the act that resulted in harm, and was this influence determinative or merely auxiliary to human action?
2. Was the risk that ultimately materialized reasonably foreseeable and preventable at the design, development, or programming stage of the system?
3. Did the human operator retain a meaningful and realistic capacity to intervene in, override, or terminate the algorithmic process at the moment when the harmful outcome became imminent?
4. At which stage of the technological lifecycle—system design, software development, manufacturing, maintenance, or operational use—did the legally relevant risk primarily originate?
5. Which actor possessed the greatest capacity to create, control, or prevent the risk that resulted in harm?

By structuring the analysis around these questions, the AMC framework provides a practical doctrinal tool for distinguishing between the layers of responsibility attributable to software developers, manufacturers, medical professionals, and healthcare institutions. Thus, the model enables courts to address the complexities of algorithmically mediated conduct while preserving the fundamental principles of criminal law concerning culpability, causation, and attribution.

Application of AMC to FDA MAUDE-reported incidents illustrates this model's necessity. In the first case (MAUDE Report No. 2955842-2025-32348), the Harmonic ACE instrument fractured during robotic liver resection while a nurse removed a clot, leaving a fragment inside the patient that was subsequently retrieved. Procedural compliance was established; no collision, misuse, or excessive force occurred; and manufacturer review identified no operator error. Thus, the breakdown originated not from surgical negligence but from latent micro-mechanical stress, vibrational tolerance, and material-fatigue dynamics embedded within the device's design and calibration logic. The locus of culpability lies within manufacturing quality assurance, not human conduct. The second case (MAUDE Report No. 2955842-2025-29306) involved bending and internal wire failure of fenestrated bipolar forceps during robotic myomectomy, resulting in a detached metal fragment that was removed intraoperatively. The surgeon complied with surgical standards, perceived no anomaly before device failure, and intervened only after functional impairment manifested. The necessity to trigger manual emergency release further demonstrates that the defect arose within servo-mechanical and software-governed control systems, not at the plane of volitional human action. The risk thus materialized in the design-maintenance continuum rather than in operative judgment (Food and Drug Administration, 2025; Fuller, Ashar, and Carey-Corrado, 2005).

In both cases, the decisive causal vector was not the surgeon's embodied agency but algorithmically mediated mechanical behavior, lifecycle maintenance parameters, and engineering tolerances beyond direct human control. The moment of risk crystallization occurred upstream of the surgical act within the design and lifecycle governance domains. Classical malpractice analysis—which presumes direct human control—is therefore structurally inadequate. Criminal liability in such contexts cannot hinge solely on the physical initiator of a procedure; instead, it must trace normative responsibility to the point at which the prohibited risk became foreseeable, preventable, and attributable to a specific technical actor. AMC thus re-anchors culpability from the surgeon-centric tradition toward a distributed responsibility framework encompassing manufacturers, software developers, and maintenance regimes, consistent with the altered architecture of modern operative causation. In doing so, AMC fills the doctrinal lacuna created by autonomous and semi-autonomous surgical systems and furnishes a technologically coherent model for evaluating culpability in the age of algorithmic medical intervention.

The AMC model does not constitute an autonomous theory of criminal liability, nor does it introduce new offence categories or replace established fault doctrines in criminal law. Its primary function is to operationalize existing criminal law concepts in cases where algorithmic systems materially intervene in the production of harm. In this respect, AMC translates abstract doctrinal notions into concrete, judicially assessable questions, such as the degree of algorithmic influence on the act, whether the relevant risk was foreseeable and preventable at the design stage, and whether meaningful human intervention was practically feasible at the time of operation.

By structuring the analysis around these questions, the AMC refines the application of existing offence types without altering their legal structure. In cases of negligent homicide, it assists in distinguishing ordinary negligence from aggravated forms of omission by clarifying the normative significance of unexercised intervention capacity. In situations involving conscious negligence, it enables courts to assess how algorithmic mediation may have affected the actor's perception of risk and, consequently, their normative

blameworthiness. Likewise, in result-aggravated offences, the AMC sharpens the evaluation of normative causation by clarifying whether the aggravated result should be attributed to the actor's conduct or differentiated across design, institutional, and operational stages. Accordingly, AMC functions as a complementary methodological framework that adapts traditional analyses of fault and causation to the realities of algorithmically mediated action without transforming the foundational structure of criminal law. Within this structure, various actors—surgeons, software developers, manufacturers, maintenance providers, and hospital administrators—contribute to the surgical outcome at different levels. In a technological environment where risk is dispersed among multiple agents and where algorithmic processes interact with human action in the execution of the surgical task, legal certainty cannot be ensured merely through administrative fines, technical safety protocols, or private-law compensation mechanisms. Consequently, the role of criminal law in the domain of robotic surgery extends beyond its traditional punitive function and assumes the character of a normative regulatory and risk-governance instrument.

According to the classical theoretical framework of criminal law, the principle of ultima ratio governs criminal sanctions as a measure of last resort. Under this principle, criminal law intervenes only where the protective mechanisms of other branches of law prove insufficient. Yet the operational architecture of systems such as Hinotori reveals a domain in which administrative sanctions and private-law remedies are inherently limited. In this context, the activation of criminal law does not amount to a violation of the ultima ratio principle; rather, it signifies a redefinition of what "last resort" entails, given the qualitative distinctiveness of technological risk.

The regulatory function of criminal law becomes particularly salient in three respects. First, criminal law normatively defines the scope of due-care obligations incumbent upon each actor: it clarifies the circumstances under which a surgeon must intervene in response to system alerts, the duties borne by software developers, the safety standards manufacturers must meet, and the maintenance cycles hospitals are required to ensure. Second, criminal law determines at which point the resulting harm should be attributed to a legally relevant actor. In cases involving algorithmic malfunctions, sensor failures, or lapses in maintenance, criminal law provides the framework through which the threshold for attributing responsibility —whether to the human operator, the software system, or institutional actors—is normatively established. Third, criminal law creates a deterrent and norm-shaping framework that limits risk-producing behavior across society; administrative sanctions or tort liability alone lack the capacity to generate such systemic preventive effects.

The proposal to expand the role of criminal law in response to technological risks has been the subject of significant debate in the literature. Among the most prominent objections is the concern that extending the scope of criminal law may lead to overcriminalization, thereby undermining the legitimacy of criminal norms. According to this view, resorting to criminal sanctions in complex and highly technical risk domains risks stretching the fault principle beyond its limits, resulting in an indeterminate diffusion of responsibility and a dilution of the deterrent effect (Beale, 2005, 758–770). In addition, critical accounts frame the expansion of criminal law partly as a problem of labeling and measurement, arguing that criminalization often obscures rather than clarifies the normative boundaries of responsibility in technologically mediated contexts (Husak, 2023, 271). Similar concerns have been raised regarding the preventive use of criminal law, which is said to conflict with its ultima ratio character and to be comparatively ineffective when measured against administrative and regulatory mechanisms (Jain, 2017, 1384). Particularly in the healthcare context, punitive responses may discourage error reporting and undermine institutional learning, rendering criminal law an ineffective tool for managing technical and systemic risks (Alghrani et al., 2024, 230–231).

Nevertheless, these objections are not sufficiently persuasive to warrant the principled exclusion of criminal law from the governance of technological risk. A common limitation of the critical literature lies in its tendency to assess criminal law through the assumption of an unbounded and undifferentiated expansion, while largely neglecting the possibility of doctrinally constrained and normatively targeted forms of criminal responsibility. In high-risk AI applications, harmful outcomes frequently result not merely from regulatory gaps but also from the failure to address foreseeable and reasonably preventable risks through adequate safety measures. Rendering such omissions entirely invisible to criminal law weakens both the fault principle and broader expectations of legal accountability (Brown, 2019, 20). Accordingly, the position advanced in this study does not support the view that criminal law should assume a general role in the management of technical risk. Rather, it argues for a limited and differentiated expansion of criminal law, directed specifically at serious breaches of duty in high-risk technological contexts. This approach rejects the automatic diffusion of criminal responsibility and instead seeks to establish a normative threshold based on foreseeability, preventability, and control capacity. Models such as AMC, which adopt a logic of differentiated attribution, exemplify how criminal responsibility may be refined rather than indiscriminately extended. Under this framework, criminal law is not positioned as a substitute for regulatory governance but as a complementary and exceptional liability regime, activated only where regulatory mechanisms fail and grave, normatively blameworthy violations occur.

In complex technological environments, such as those involving Hinotori robotic surgical systems—where human life is directly implicated and where harmful outcomes may stem not only from individual fault but also from systemic design choices and institutional processes—the intervention of criminal law becomes essential for closing normative gaps, delineating the architecture of the act, and generating preventive force. Thus, in the context of interventions performed with Hinotori and similar robotic systems, criminal law functions not merely as an ex post mechanism reacting to harmful outcomes but as a legal instrument that structures the limits of risk generation and constructs the normative order of technologically mediated medical practice.

In this regard, the partial adaptation of traditional criminal law doctrines is insufficient. The multi-agent, technically complex nature of robotic and AI-assisted medical systems requires the establishment of an entirely new legislative framework—one that clearly delineates spheres of responsibility and articulates sanctions with unambiguous precision, leaving no room for uncertainty in the governance of high-risk medical technologies.

IV. Conclusion

The Hinotori surgical robot, whose use is increasing instantly, has many identified advantages, but it is also important to determine what 'possible' risks it evokes, so it is important to balance the innovative initiative with safety interests. In order to protect patients and reduce the risk of malpractice liability for doctors who choose to exploit the potential of the Hinotori for surgical applications, as well as to realistically define the criminal liability of hospitals, manufacturers, suppliers, and software programmers, it is necessary to implement effective modern and innovative legal regulations, not to integrate the provisions applicable to such robots into traditional laws.

This study demonstrates, through an in-depth analysis centered on the Hinotori robotic surgery system, that the challenges posed by algorithmically mediated harm cannot be adequately addressed through abstract or purely technical discussions. The examined context reveals that, in high-risk AI applications, harmful outcomes rarely arise from a single human action; rather, they emerge from the combined interaction of system design, software architecture, institutional organization, and operational practice. This

structural complexity exposes the limitations of traditional, strictly individual-centered approaches to criminal liability and underscores the need for a more differentiated doctrinal assessment.

Against this background, AMC model developed in this study is not merely an explanatory framework but provides a normatively actionable basis for concrete doctrinal and policy development in criminal law. First, effective criminal-law assessment of harm in algorithmically intensive systems presupposes the availability of reliable ex post reconstruction of decision-making processes. This finding supports the introduction of targeted obligations to preserve system logs and report serious incidents or anomalous deviations for AI systems exceeding a defined risk threshold, thereby enhancing the practical assessability of causation.

Second, the AMC framework clarifies that criminal fault cannot be confined to conduct at the moment of use. Instead, it highlights that security- and safety-oriented design choices—such as validation procedures, continuous monitoring, update mechanisms, warning systems, and meaningful override capacities—constitute legally relevant domains of due care. The presence or absence of such measures becomes a decisive factor in evaluating whether risk was normatively avoidable, and thus whether criminal negligence can be attributed beyond the operational level.

Finally, the analysis indicates that the application of a uniform negligence standard to high-risk AI systems fails to capture the differentiated risk profiles inherent in algorithmically mediated action. By structuring the assessment around algorithmic impact, preventability, and control capacity, AMC provides a principled basis for discussing a graduated negligence framework tailored to high-risk AI contexts without altering the statutory structure of existing offences. In this respect, AMC does not propose an autonomous liability regime but offers a doctrinally grounded normative framework capable of adapting established concepts of causation and fault to the operational realities of advanced algorithmic systems while simultaneously informing future regulatory and policy choices.

If, at some future stage, any form of legal personality were to be conferred upon robotic or artificial intelligence systems, assessing their criminal responsibility according to the criteria developed for fully capable human agents would be dogmatically untenable. This analysis conceptualizes any prospective liability framework solely by analogy to the model of limited criminal capacity applied to minors. Because AI systems do not possess the volitional direction, evaluative judgment, or cognitive capacity to grasp the normative significance of their actions, their criminal responsibility could be determined only with reference to the foreseeability of their technical operations, the degree of their dependence on human oversight, and the structural limits of their computational architecture. In this sense, robotic systems should not be regarded as "full-fledged offenders," but rather as functional entities endowed with a form of constrained and conditional criminal capacity, a characterization that offers the greatest normative coherence within technologically mediated environments.

V. Recommendations and the Perspectives of the Future

The application of traditional laws to robots cannot be expected to follow the spirit of innovation in terms of effective judgment and determination of liability. The biggest problem at this point is the lack of specific and modern legal regulations to attribute a legal status to AI and robots. Provision of this determination may help facilitate the adaptation of different areas of law to technological progress and safe use (Kuklinska, 2021, 18). In this case, the first step in the regulations to be made will be to determine the legal personality status of Hinotori and other medical robots.

Although robotic and AI-assisted surgical systems have not yet been granted any form of legal personality, their identification and traceability remain indispensable for establishing a coherent framework of

responsibility. The absence of legal personhood does not eliminate the structural necessity for Hinotori—and its software iterations—to be uniquely identifiable, continuously monitored, and forensically traceable. For this reason, a mandatory registration and certification regime should be established, whereby all robotic surgical systems are entered into a centralized regulatory database, assigned unique digital identifiers, and subjected to periodic certification in accordance with evolving safety and technical standards.

In high-risk AI systems, proposed registration and certification regimes should be understood not merely as administrative oversight tools but as normative thresholds that define foreseeability, preventability, and the scope of legally relevant duties of care in criminal law. By specifying which risks are legally salient for particular actors, such mechanisms establish the analytical foundation for fault assessment. Within this framework, the boundaries of criminal responsibility should not be drawn according to abstract role descriptions but rather according to concrete risk domains and the actor's effective capacity for control and intervention. Accordingly, manufacturers and system designers are subject to criminal evaluation in relation to design-level risks, including system architecture, validation processes, and safety-by-design measures; software developers in relation to safety-relevant algorithmic modifications; operators and surgeons in relation to professional duties of care during system operation where meaningful human intervention is feasible; and hospitals in relation to institutional risk governance through training, protocols, and supervision. The Algorithmic-Mediated Causation (AMC) model operationalizes this allocation by jointly assessing algorithmic impact intensity, risk preventability, and control capacity for each actor, rendering governance measures concrete, differentiated, and normatively justifiable from a criminal-law perspective.

Furthermore, it should be ensured that clear lines should be drawn in terms of the obligations and sharing of criminal liability of potential actors, namely, manufacturers, software programmers, surgeons, and hospitals. These regulations should also include international standards for the design, production, testing, and use of Hinotori and procedures for certification processes. In particular, clear rules and sanctions should be introduced for data security, provision of informed consent, and transparency of artificial intelligence algorithms within the scope of personal data protection. Along with criminal liability and sanctions, it is equally important to explain the rules regarding compensation for the damage incurred. In addition, ethics committees should be established, and when Hinotori commits an offence, an independent party's audit should be made mandatory in the judicial processes.

Peer Review Externally peer-reviewed.
Conflict of Interest The authors has no conflict of interest to declare.
Grant Support The authors declared that this study has received no financial support.

Author Details
Esra Nur Bal (Ph.D. student)
[1] Uskudar University, Institute of Addiction and Forensic Sciences, İstanbul, Türkiye
0000-0001-7354-4584 esranur.bal@st.uskudar.edu.tr

Mohammad Abualrob (Ph.D., Assistant Professor)
[2] Lusail University, College of Law, Doha-Qatar
0000-0001-5296-7473

Bibliography

Abdelaziz, D. K. A. (2025). Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. *Journal of Infrastructure, Policy and Development, 9*.

Akbaba, T. (2021). *Türk Ceza Hukukunda Nedensellik Bağı.* (Yüksek Lisans Tezi). İstanbul Ticaret Üniversitesi.

Alemzadeh, H., Raman, J., Leveson, N., Kalbarczyk, Z., & Iyer, R. K. (2016). Adverse events in robotic surgery: A retrospective study of 14 years of FDA data. *PLOS ONE*, *11*(4), e0151470. doi: 10.1371/journal.pone.0151470.

Alghrani, A., Rehman, U., Sarwar, M. S., & Brennan, P. A. (2024). Balancing the scales of safety: The criminal law's impact on patient safety and error reduction. *British Journal of Oral and Maxillofacial Surgery, 62*(3), 229–232. doi: 10.1016/j.bjoms.2023.11.018.

Bal, E. N., & Sarıbey, A. Y. (2025). Artificial intelligence in forensic science: Applications, legal framework and criminal liability regime. In *2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)* (pp. 1–7). IEEE. doi: 10.1109/ACDSA65407.2025.11165965.

Beale, S. S. (2005). The many faces of overcriminalization: From morals and mattress tags to overfederalization. *American University Law Review, 54*, 747–780.

Beard, T. R., Ford, G. S., Koutsky, T. M., & Spiwak, L. J. (2009). Tort liability for software developers: A law & economics perspective. *John Marshall Journal of Computer & Information Law*, *27*(2), 199–234.

Boğa, B. (2024). *Olası kast–bilinçli taksir ayrımının teorik temelleri* (Doktora tezi). Ankara Hacı Bayram Veli Üniversitesi, Lisansüstü Eğitim Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Ceza ve Ceza Muhakemesi Hukuku Bilim Dalı.

Boscarato, C. (2011). Who is responsible for a robot's actions? An initial examination of Italian law with a European perspective. In B. van den Berg & L. Klaming (Eds.), *Technologies on the Stand: Legal and Ethical Questions in Neuroscience and Robotics* (pp. 393–408). Nijmegen: Wolf Legal Publishers.

Brown, D. K. (2009). Can criminal law be controlled, *Michigan Law Review, 108*, 1–2.

Centel, N., Zafer, H., & Çakmut, Ö. (2005). *Türk Ceza Hukukuna Giriş* (3rd ed.). Beta Yayıncılık.

De Micco, F., Grassi, S., Tomassini, L., Di Palma, G., Ricchezze, G., & Scendoni, R. (2024). Robotics and AI into healthcare from the perspective of European regulation: Who is responsible for medical malpractice. *Frontiers in Medicine*, *11*, 1428504. doi: 10.3389/fmed.2024.1428504.

Dharm, J., Girme, A., & Gharde, U. (2024). Artificial intelligence: Challenges in criminal and civil liability. *International Journal of Law, 10*(2), 52–57.

Dönmezer, S. (2003). *Genel Ceza Hukuku Dersleri*. Bahçeşehir Üniversitesi Yayınları.

Ebihara, Y., Hirano, S., Kurashima, Y., Takano, H., Okamura, K., Murakami, S., Shichinohe, T., Morohashi, H., Oki, E., Hakamada, K., Ikeda, N., & Mori, M. (2024). Tele-robotic distal gastrectomy with lymph node dissection on a cadaver. *Asian Journal of Endoscopic Surgery*, *17*(1). doi: 10.1111/ases.13246.

Fernández Llorca, D., Charisi, V., Hamon, R., Sánchez, I., & Gómez, E. (2023). Liability regimes in the age of AI: A use-case driven analysis of the burden of proof. *Journal of Artificial Intelligence Research, 76*, 613–644. doi: 10.48550/arXiv.2211.01817.

Filipova I.A., & Koroteev V.D. (2023). Future of artificial intelligence: Object of law or legal personality? *Journal of Digital Technologies and Law*, *1*(2), 359–386. doi: 10.21202/jdtl.2023.15.

Food and Drug Administration. (2025). *Manufacturer and User Facility Device Experience database.* https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/textsearch.cfm.

Fuller, J., Ashar, B. S., & Carey-Corrado, J. (2005). Trocar-associated injuries and fatalities: An analysis of 1,399 reports to the FDA. *Journal of Minimally Invasive Gynecology, 12*(4), 302–307. doi: 10.1016/j.jmig.2005.05.008.

Giannini, A., & Kwik, J. (2023). Negligence Failures and Negligence Fixes. A Comparative Analysis of Criminal Regulation of AI and Autonomous Vehicles. *Criminal Law Forum, 34,* 43–85. doi: 10.1007/s10609-023-09451-1.

Gordon, W.J., Ikoma, N., Lyu, H., Jackson, G.P., & Landman, A. (2022). Protecting procedural care—cybersecurity considerations for robotic surgery. *Npj Digital Medicine, 5*, 148. doi: 10.1038/s41746-022-00693-8.

Gökpınar, M. (2008). Ceza sorumluluğunun temeli: Kast. *TBB Dergisi, 21*(79), 198–234.

Hakeri, H. (2015). *Ceza hukuku Genel Hükümler* (18. bs.). Adalet Yayınevi.

Holder, C., Khurana, V., Harrison, F., & Jacobs, L. (2016). Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II). *Computer Law & Security Review*, *32*(3), 382–402. doi: 10.1016/j.clsr.2016.03.001.

Husak, D. (2022). Retributivism and over-punishment. *Law and Philosophy, 41*, 169–191. doi: 10.1007/s10982-021-09422-w.

Husak, D. (2023). Six questions about overcriminalization. *Annual Review of Criminology, 6*, 265–284.

Ichino, M., Sasaki, H., Takenaka, M., Zennami, K., Takahara, K., & Shiroki, R. (2024). Robotic-assisted sacrocolpopexy with hinotori, a brand-new surgical robot system produced in Japan; report of initial clinical case series. *Asian Journal of Endoscopic Surgery*, *17*(4). doi: 10.1111/ases.13380.

Ide, H. (2024). Revolutionary advances of robotic surgery in the urology field. *Juntendo Medical Journal*, *70*(3), 230–238. doi: 10.14789/jmj.jmj24-0008-r.

Jain, E. (2017). *Capitalizing on criminal justice*. *Duke Law Journal, 67*, 1381–1431.

Kan, C. H. (2024). Criminal liability of artificial intelligence from the perspective of criminal law: An evaluation in the context of the general theory of crime and fundamental principles. *International Journal of Eurasia Social Sciences*, *15*(55), 276–313. doi: 10.35826/ijoess.4434.

Katsuno, H., Morohara, K., Endo, T., Chikaishi, Y., Kikuchi, K., Nakamura, K., Matsuo, K., Higashiguchi, T., Koide, T., Hanai, T., & Morise, Z. (2024). A new era in surgical oncology: Preliminary insights into the hinotori™ surgical robot system's role in rectal surgery using the double bipolar method. *World Journal of Surgical Oncology*, *22*(1), 215. doi: 10.1186/s12957-024-03499-y.

Kawasaki Heavy Industries. (2021, July 31). How AI is changing society: Responsibility and ethics for connected future. *Kawasaki Heavy Industries*. https://answers.khi.co.jp/en/connected-society/20210731e-05/.

Kitatsuji, H. (2023). Hinotori surgical robot system: The made-in Japan robotic-assisted surgery system. *Journal of the Japanese Society of Medical Imaging and Information Sciences*, *40*(2), 20–23.

Kitatsuji, H., Ura, H., Ueda, T., Usuki, Y., Tojo, T., Yamamori, H., & Doi, W. (2022). *Hinotori surgical robot system, the first made-in Japan robotic-assisted surgery system*. *Kawasaki Technical Review*, *183*, 9–14.

Kowert, W. (2017). The foreseeability of human-artificial intelligence interactions. *Texas Law Review*, *96*, 181-204.

Köken, E. (2021). Criminal liability of artificial intelligence. *Türkiye Adalet Akademisi Dergisi*, *12*(47), 247–286.

Kuklińska, L. A. (2021, September 6). *Establishing liability for the actions of artificial intelligence: Recommendation for the European Commission*. Institute of New Europe. https://ine.org.pl/en/establishing-liability-for-the-actions-of-artificial-intelligence-recommendation-for-the-european-commission/

Kuromatsu, I., Inaba, S., Nakano, S., Yamada, T., & Yamada, Y. (2024). Experience in implementing and operating Hinotori–Da Vinci: From a team without prior Da Vinci experience. *Japanese Journal of Endourology and Robotics*, *37*(1), 55–59. doi: 10.11302/jserjje.37.1_55.

Lewna, A. (2023). The construct of strict liability in criminal law of England and Wales in the context of Polish legal regulations on the subjective element in the structure of a prohibited act. *Studia Iuridica Lublinensia*, 32(2), 203–223.

Louis, M., Fernandez, A. A., Manap, N., Kandasamy, S., & Lee, S. (2021). Artificial intelligence: Is it a threat or an opportunity based on its legal personality and criminal liability? Journal of Information System and Technology Management, 6, 1–9. doi: 10.35631/JISTM.620001.

Loveless, J., Allen, M., & Derry, C. (2020). *Complete criminal law: Text, cases, and materials* (7th ed.). Oxford University Press.

Mantovani, F. (2008). Colpa. In *Umanità e razionalità del diritto penale* (pp. 359–378). Cedam.

Marcus, H. J., Ramirez, P. T., Khan, D. Z., Horsfall, H., Hanrahan, J. G., Williams, S. C., Beard, D. J., Bhat, R., Catchpole, K., Cook, A., Hutchison, K., Martin, J., Melvin, T., Stoyanov, D., Rovers, M., Raison, N., Dasgupta, P., Noonan, D., Stocken, D., ... The IDEAL Robotics Colloquium. (2024). The IDEAL framework for surgical robotics: Development, comparative evaluation, and long-term monitoring. *Nature Medicine, 30*(1), 61-75. doi: 10.1038/s41591-023-02732-7.

Matsuo, T. (2018). Criminal and civil liability of medical AI and robots. *Law & Practice*, *12*, 83–106.

Medicaroid. (2021). Medical robotic solutions that help everyone live healthier, more peaceful lives. *Surgical Robotics Technology*. https://www.surgicalroboticstechnology.com/company/medicaroid/.

Miyo, M., Okita, K., Okuya, K., Ito, T., Akizuki, E., Ogawa, T., Ishii, M., Miura, R., Ichihara, M., Korai, T., Kimura, A., & Takemasa, I. (2023). Right hemicolectomy for ascending colon cancer using the hinotori surgical robot system: The first ever case report for colon cancer. *Asian Journal of Endoscopic Surgery*, *16*(3), 604–607. doi: 10.1111/ases.13197.

Motoyama, D., Matsushita, Y., Watanabe, H., Tamura, K., Otsuka, A., Fujisawa, M., & Miyake, H. (2023). Robot-assisted adrenalectomy using a Hinotori surgical robot system: Report of first series of six cases. *Asian Journal of Endoscopic Surgery*, *16*(3), 489–495. doi: 10.1111/ases.13212

Öztürk, M. K. (2023). Türk Ceza Kanunu'nda bir iştirak şekli olarak faillik (TCK m. 37). *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, *13*(1), 255–307. doi: 10.52273/sduhfd..1220467.

Pagallo, U. (2011). Killers, fridges, and slaves: A legal journey in robotics. *AI & Society, 26*(4), 347–354. doi: 10.1007/s00146-010-0316-0.

Parlak Börü, Ş. (2019). Robotik cerrahi müdahalelerden doğan hukuki sorumluluk. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, *10*(2), 758–775. doi: 10.21492/inuhfd.636507.

Parsons, S. (2004). Intention in criminal law. *Mountbatten Journal of Legal Studies*, 4(1), 2, 5-19.

Pepito, J. A., Vazquez, B. A., & Locsin, R. C. (2019). Artificial intelligence and autonomous machines: Influences, consequences, and dilemmas in human care. *Health*, *11*(7), 932–949. doi: 10.4236/health.2019.117075.

Pinkevich, T., & Konev, D. (2024). The risks of Using Artificial Intelligence As A Tool and Means of Committing Offences: Problems of Legal Regulation and Ways of Counteracting Them. *Legal Order: History, Theory, Practice, 2*(16), 84-94. doi: 10.47475/2311-696x-2024-43-4-148-153.

Rathnayake, A. P. (2024). Legal and ethical facets of robotic surgery: A suggestion for a guideline. *Sri Lanka Journal of Forensic Medicine, Science & Law*, *15*(1), 29–33. doi: 10.4038/sljfmsl.v15i1.7947.

Razek, R. M. A. M. A. (2024). Criminal responsibility for errors committed by medical robots: Legal and ethical challenges. *Journal of Law and Sustainable Development*, *12*(1), 1–20. doi: 10.55908/sdgs.v12i1.2443.

Reinach, A. (2009). On the concept of causality in the criminal law. *Libertarian Papers*, *1*, 35. doi: 10.2139/ssrn.1356054.

Rivero-Moreno, Y., Echevarria, S., Vidal-Valderrama, C., Pianetti, L., Cordova-Guilarte, J., Navarro-Gonzalez, J., Acevedo-Rodriguez, J., Dorado-Avila, G., Osorio-Romero, L., Chavez-Campos, C., & Acero-Alvarracín, K. (2023). Robotic surgery: A comprehensive review of the literature and current trends. *Cureus*, *15*(7), e42370. doi: 10.7759/cureus.42370.

Robinson, P. H. (1993). Functional analysis of criminal law. *Northwestern University Law Review*, *88*, 857–913.

Simester, A. P. (2021). *Fundamentals of criminal law: Responsibility, culpability, and wrongdoing*. Oxford University Press.

Suzuki, Y., Sato, H., & Nakazawa, N. (2023). Current status of robotic surgery in Japan gynecologic field. *Intelligent Surgery*, *6*, 25–30. doi: 10.1016/j.isurg.2023.03.001.

Şenol, F. (2025). Kasten yaralama sonucu ölüme neden olma suçunda nedensellik ve objektif isnadiyet. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, *74*(1), 199–271.

Taymur, B. (2024). Kast ve Bilinçli Taksirin Haksızlık Yoğunluklarının İncelenmesi. *Kırklareli Üniversitesi Hukuk Fakültesi Dergisi*, *2*(2), 353-394.

Tervoort, T., De Oliveira, M. T., Pieters, W., Van Gelder, P., Olabarriaga, S. D., & Marquering, H. (2020). Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: A scoping review. *IEEE Access, 8*, 84352–84361. doi: 10.1109/ACCESS.2020.2984376.

Tobe, T., Terakawa, T., Ueki, H., Hara, T., Shiraishi, Y., Wakita, N., Okamura, Y., Suzuki, K., Bando, Y., Chiba, K., Teishima, J., Nakano, Y., & Miyake, H. (2024). Initial experience of robot-assisted laparoscopic pyeloplasty for ureteropelvic junction obstruction using the Hinotori Surgical Robot System. *International Journal of Medical Robotics and Computer Assisted Surgery*, *20*(5), e2673. doi: 10.1002/rcs.2673.

Tomihara, K., Ide, T., Ito, K., Tanaka, T., & Noshiro, H. (2024). Robotic spleen-preserving distal pancreatectomy using the first domestic surgical robot platform (the hinotori™ Surgical Robot System): A case report. *Surgical Case Reports*, *10*(1), 22. doi: 10.1186/s40792-024-01808-x.

Vuletić, I., & Petrašević, T. (2020). Is it time to consider EU criminal law rules on robotics. *Croatian Yearbook of European Law and Policy*, *16*, 225–244.

Vulpe, A., Crăciunescu, R., Drăgulinescu, A.-M., Kyriazakos, S., Paikan, A., & Ziafati, P. (2021). Enabling Security Services in Socially Assistive Robot Scenarios for Healthcare Applications. *Sensors*, *21*(20), 6912. doi: 10.3390/s21206912.

Walden, P. A., Zeybek, B., & Phelps, J. Y. (2018). Understanding the legal essentials of a bowel injury lawsuit in minimally invasive gynecologic surgery. *Journal of Minimally Invasive Gynecology*, *25*(1), 30–37. doi: 10.1016/j.jmig.2017.09.018.

Wasserstrom, R. A. (1960). Strict liability in the criminal law. *Stanford Law Review*, 12(4), 731–745.

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115–158. doi: 10.1007/s10207-021-00545-8.

Ziemianin, K. (2021). Civil legal personality of artificial intelligence. Future or utopia? *Internet Policy Review*, *10*(2), 1544-1563. doi: 10.14763/2021.2.1544.