International Journal of Research and Review
[Indexed, Peer-Reviewed Journal]
Volume 12; Issue: 10; October 2025
Website: www.ijrrjournal.com
Review Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Autonomous Systems (AI) and Criminal Imputability: Challenges for Modern Law

Enrico Moch, PhD

Academic Director, Department of Laws, GrandEdu Research School, Germany

Corresponding Author: Dr Enrico Moch, E-Mail: Enrico.Mocch@GrandEduResearchschool.de

DOI: https://doi.org/10.52403/ijrr.20251029

ABSTRACT

Autonomous systems are changing the foundations of criminal liability. Where machines act autonomously, normative gaps arise that put the principle of culpability to a new test. This paper explores the question of how criminal imputability can be reconstructed under the conditions of technical autonomy. It pursues the goal of determining the prerequisites of a criminal law that can react to autonomous systems without losing its normative identity. The study follows a comparative dogmatic methodology. It combines classical legal analysis with interdisciplinary approaches to reflection and is based on contrasting case studies in the fields of transport, medicine and the military. These sectors are exemplary for high-risk areas in which technical systems directly intervene in protected legal interests and thus enable generalisable statements about responsibility and guilt. The results show that criminal imputability remains possible even in the age of artificial autonomy if it is normatively re-anchored by preventive structures. The basis remains action, causality, intent, negligence and culpability, supplemented by organisational obligations, auditability and verifiability. The AI Act and the Product Liability Directive 2024 create the framework for preventive responsibility at European level. Internationally, human rights standards, in particular Article 1 GG, Article 2 ECHR and Article 36 ZP I, ensure the legitimacy of this order. Criminal law retains its authority if it makes responsibility visible, enforces transparency and upholds human dignity as the limit of technical power to act. It remains the guarantor of human freedom in an increasingly automated world.

Keywords: Autonomous systems; imputability under criminal law; artificial intelligence; culpability principle; organisational responsibility; responsibility gap; auditability; human dignity; international regulation; AI Act

1 INTRODUCTION

Autonomous systems present criminal law with one of its most profound tests. Where machines make decisions autonomously, zones of normative uncertainty arise. The classic logic of attribution, based on action, intent and guilt, is shaken when decisions are made by learning systems whose functioning is only comprehensible to a limited extent, even to experts. This shifts the centre of criminal responsibility. It no longer lies solely in the individual act of will, but in the organisation of technical power.

This shift affects the foundation of the rule of law. The principle of guilt is not just a dogma of criminal law, but an expression of an idea of responsibility that sees people as acting, understanding and taking responsibility for their actions. However, when systems act without intending to and produce effects without understanding, a responsibility gap arises. This gap threatens not only dogmatics,

but also trust in the ability of law to bind technical development normatively.

This study examines the question of how criminal accountability can be reconstructed under the conditions of technical autonomy. It does not seek a fusion of man and machine, but rather a standard that preserves human responsibility in a digitalised world. The aim is to determine the prerequisites for a criminal law that can react to autonomous systems without losing its own normative identity.

The focus is on analysing the existing liability and attribution models of German criminal law and their transferability to European and international levels. Building on this, case studies from the fields of transport, medicine and the military are used as examples to show how responsibility shifts along different levels of technical complexity. In addition, ethical and human rights guidelines are included to prevent efficiency from becoming a substitute for legitimacy.

Criminal law is thus at a threshold. It must learn not only to regulate technical systems, but also to integrate them into its own conceptual world. Only if action, guilt and dignity remain in a new balance can it assert its authority. The following sections therefore develop a methodological framework in which dogmatic rigour, interdisciplinary reflection and normative creative power are combined.

The problem areas outlined above make it clear that criminal law operates in a field of tension between technical autonomy and legal responsibility. In order to capture this dynamic precisely, a clear methodological framework is required that combines the systematic, comparative law and normative dimensions of the topic.

1.1 Methodology and research framework

This study follows a dogmatic-comparative methodology that combines classic instruments of legal analysis with interdisciplinary approaches to reflection. The aim is not to describe technical processes, but to categorise them in legal and normative terms. The starting point is the question of how imputability under the conditions of technical autonomy can be reconstructed under the rule of law. The current criminal law, i.e. de lege lata, is systematically analysed and at the same time supplemented by legal policy perspectives, i.e. de lege ferenda.

The dogmatic method serves to clarify normative structures. Action, causality, intent, negligence and guilt form the framework against which new phenomena of technical autonomy are reflected. The comparative law approach extends this analysis to European and international levels. The AI Act, the Product Liability Directive 2024 and Article 36 ZP I are used as reference points for preventive responsibility architectures in order to examine the compatibility of criminal law categories in multi-layered legal areas.

The case selection includes transport, medicine and the military and follows an analytical principle. These three sectors represent high-risk areas of technical autonomy in which autonomous systems directly interfere with protected legal interests.

They allow generalisable statements to be made because they reveal different levels of responsibility. Individual control is evident in traffic, shared responsibility between man and machine in medicine, and the institutionalised decision-making structure in the military. The contrasts between these fields illustrate how normative responsibility structures shift depending on the technical and organisational density.

This is supplemented by a critical integration of literature that takes into account economic, ethical and socio-technical counter-positions. These include Bryson (2018), Yeung (2019), Hagendorff (2020) and Helm and Gerlek (2025). This integration serves as a theoretical validation and examines whether legal attribution models remain viable even where responsibility diffuses in networks or is absorbed by governance mechanisms.

The work combines dogmatic rigour with interdisciplinary depth. It understands criminal law not merely as a reacting, but as a normative organising authority. Its legitimacy is measured by keeping responsibility visible and verifiable, even when actions arise from autonomous systems.

2 Explanation of terms

The discussion about autonomous systems in criminal law is characterised by conceptual vagueness. Technical, philosophical and legal levels often overlap without being clearly differentiated from one another. Questions of responsibility become blurred as a result. A viable analysis therefore starts with the language and the precise definition of what autonomy and attribution actually mean. Autonomy in the technical sense refers to the ability of a system to make decisions independently within defined framework conditions. It is based on machine learning methods and adaptive algorithms. Such systems process input data, recognise patterns and derive options for action from them. The decisive factor is not how "intelligent" a system appears, but whether its decisions are legally relevant. In terms of criminal law, it only counts if autonomous behaviour has direct consequences for protected legal interests (Feldmann 2024; Hilgendorf 2018).

Attributability under criminal law is traditionally linked to human behaviour. It presupposes intent or negligence, i.e. culpable behaviour that violates a criminal provision. The basis is the normative network of action, causality, fault and culpability. This network becomes fragile when systems produce results that cannot be clearly attributed to any individual (Cuccuru 2025; Globke 2021). The causal series remains technically comprehensible, but dogmatically a vacuum is created. Nobody acts, and yet an attribution deficit arises in algorithmic systems.

The so-called responsibility gap describes this break: damage occurs, but the person responsible remains invisible (Zamani 2025). Responsibility breaks down into sub-areas of development, operation and use without anyone controlling the overall process (Pane & Permana 2025; Moafa & Almarri 2025). Criminal law is thus faced with a new complexity that overtaxes its traditional offender logic. Attribution is more than technical causality; it is a legally mediated relationship between duty and action. §§ Sections 13 and 14 of the German Criminal Code make it clear that responsibility arises where a guarantor position or acting on behalf of others is legally justified. For autonomous systems, this means that the person who controls the design, training and use of the system remains responsible, not the machine itself. In addition, there are organisational and monitoring obligations, which Münster (2022) and Thöne (2020) describe as central guarantor obligations in the digital context.

The distinction from civil law illustrates the special nature of this situation. While tort and product liability law recognise collective risk allocation (Sommer 2020; Körber & Koenig 2020), criminal law remains person-related. It requires individual guilt and normatively mediated action. The dogmatic sharpness of the current debate lies in this difference. Here, concepts become boundary lines that determine whether criminal law can maintain its binding force or loses its validity in the structures of technical autonomy.

European Union law also requires precise terminology. Article 3(1) of the European Union's AI Act defines a machine-based system that operates with varying degrees of autonomy and generates predictions, recommendations or decisions for specific goals that can influence real or virtual environments. Art. 4 para. 1 differentiates between risk classes, an approach that also marks a threshold of relevance under criminal law. Relevance arises where autonomous decisions interfere with the protection of legal interests. The AI Act is therefore not linked to technical complexity, but to functional relevance. In legal terms, it is the effect that counts, not the architecture of the algorithm.

In addition, Articles 1, 7 and 8 of the Charter of Fundamental Rights of the European Union enshrine key protected rights: human dignity, privacy and data protection. They are also binding on private individuals. This horizontal effect gives them indirect significance under criminal law, as they form the standard for duties of care and organisation. Anyone who develops or uses AI systems is responsible for ensuring that these rights are not violated. European terminology distinguishes between

- technical autonomy; the operational decision-making ability of the system,
- regulatory autonomy; the Member States' room for manoeuvre, and
- legal autonomy; accountability in the sense of the principle of culpability.

This poses a double challenge for criminal law. National imputability standards (Sections 13, 14 of the German Criminal Code) must be linked with transparency, documentation and fundamental rights obligations under EU law in such a way that both provability and the protection of fundamental rights are guaranteed. Only this link makes it possible to think consistently about imputability not only nationally, but also in the European and international discourse.

3. Analysis Of Existing Liability Models

Criminal law is based on the classic elements of offence, causality, intent, negligence and culpability. This structure remains valid as long as human behaviour is at the centre. However, autonomous systems shift this structure. Their own decisions cannot be directly linked to human forms of intent or negligence and thus create systematic gaps. Criminal law has historically operated with a personal logic of attribution: responsibility is linked to conscious, intentional behaviour. Autonomous systems, on the other hand, produce outcomes that are technically determinable but hardly traceable in normative terms. This is where the tension between traditional dogmatism and digital complexity begins. This analysis makes a strict distinction between current law (de lege lata) and reform options (de lege ferenda).

3.1 The model of individual guilt

The principle of guilt forms the core of German criminal law. Criminal liability presupposes personally reproachable behaviour (§§ 13, 15 StGB). Autonomous systems possess neither consciousness nor insight; they lack the capacity for normative self-determination. It is therefore impossible to transfer human characteristics of the offence to machine processes. The fiction of an "electronic person" discussed in the literature (Gruber et al. 2015; Hilgendorf 2018) is untenable because it abandons the personal basis of the principle of culpability. Criminal liability can only apply to natural persons who are responsible for design, monitoring or use.

3.2 Producer and operator liability

Producer liability is enshrined in German civil law (Section 823 BGB; Product Liability Act). Criminal law relevance arises if a specific duty of care subject to criminal prosecution is breached (negligence offences pursuant to Sections 222, 229 of the German Criminal Code). In the case of learning systems, the risk shifts to the phase after commissioning: errors can arise through updates, training data or self-adaptive behaviour. Civil law is linked to the defect of a product, not to organisational or monitoring obligations. Therefore, it is not the technical defect that is relevant under criminal law, but the failure to supervise, test or ensure safety. At European level, the AI Act and the planned Product Liability Directive 2024 introduce binding documentation and verification obligations. They are conceived under administrative and civil law, but have an indirect effect under criminal law because they define standards for dutiful behaviour. In future, a breach of transparency or audit obligations may be assessed as an objective breach of due diligence.

3.3 Organisational culpability and corporate responsibility

German criminal law does not recognise an independent corporate criminal law. De lege lata, the liability of legal persons is mediated via Section 30 OWiG and Section 130 OWiG. Fines can be imposed if managers commit criminal offences or administrative offences or violate their supervisory duties. However, these regulations are proving to be inadequate for highly complex AI systems that operate within distributed development and deployment structures.

Organisational culpability becomes the central point of reference: responsibility arises where risk and control structures are insufficiently defined or documented. De lege ferenda, a more comprehensive corporate sanction law is required that explicitly covers structural breaches of duty. Essers (2024) and Sommer (2020) emphasise that only such a system can effectively standardise organisational obligations in safety-critical AI applications.

The European AI Act provides the preventive infrastructure for this by establishing auditability and risk management as standard obligations. There are parallels internationally:

- In the USA, the Caremark Doctrine obliges company boards to set up control systems for mission-critical risks (In re Caremark Int. Inc., 1996).
- In international law, Art. 36 ZP I establishes a state obligation to carry out a preliminary examination of new technologies as a collective organisational obligation at state level.

These models illustrate that responsibility is shifting from the individual act to structures of control.

3.4 Hybrid models and preventive attribution

Hybrid models combine individual and organisational responsibility. They operate with preventive instruments such as audit obligations, transparency requirements and extended due diligence requirements for developers, operators and users (Pane & Permana 2025; Zamani 2025). As a result, accountability is no longer established exclusively retrospectively, but is secured preventively through regulatory architectures. Catalogues of obligations define in advance who has to take which measures, set up which controls and provide which evidence. This also changes the function of the elements of the offence: Acts and causality remain the basis, but are concretised through the obligation to fulfil duties. Attribution does not only take place retrospectively, but also through compliance with normative horizons of expectation. Only if duties are clearly formulated, documented and verifiable will the principle of fault remain practically enforceable.

3.5 Interim conclusion

No existing model is sufficient on its own. Criminal law must combine classic categories with new liability logics. Only if prevention, organisational duties and individual responsibility are combined into a coherent system will criminal law remain capable of acting in the age of automated autonomy. A multi-level structure is created:

- **national** → guilt and individual responsibility,
- **European** → preventive catalogues of obligations and auditability,
- **international** → minimum standards under human rights and international law.

This connection forms the dogmatic basis on which the following case analyses (Chapter 4) are built.

4 Case analyses

The case studies show how autonomous systems claim the classic elements of criminal law. The decisive factors are action, causality, objective attribution, intent or negligence and culpability. Three fields of application - self-driving vehicles, robotic surgery and autonomous weapons systems - are analysed in order to illustrate where current law reaches its limits and which normative adjustments are required.

4.1 Self-driving vehicles

De lege lata, the driver remains the norm addressee according to Section 7 StVG and Sections 222, 229 StGB as long as he can exert a de facto influence on the vehicle. Case law (Darmstadt Regional Court 2022; Munich Regional Court I 2022) confirms this line: the driver remains the legal "master of the system", even if technical control elements are largely automated. This means that the principle of fault threatens to lose its factual basis if there is no longer any real possibility of control. The Federal Court of Justice has already emphasised in the pacemaker case (BGHSt 29, 317) that criminal responsibility can be shifted to upstream phases of design, maintenance and monitoring. For highly automated vehicles, this means that attribution must not end with the driver, but must include the levels of responsibility of developers, integrators and operators, especially where testing and safety structures are lacking.

The European AI Act concretises this responsibility: manufacturers must design systems in such a way that decisions remain traceable and verifiable (auditability). A breach of this obligation can be indirectly categorised as negligence. De lege ferenda, the obligation to auditability should be expressly codified as an organisational obligation relevant under criminal law.

4.2 Robotic surgery

In the area of robotic assistance systems, the doctor remains criminally liable de lege lata. According to the established case law of the Federal Court of Justice (VI ZR 204/09), a lack of information, incorrect monitoring or organisational deficits justify criminal liability for negligence. This principle applies as long as human action and supervision remain comprehensible. However, problems of proof arise with increasing system autonomy. If the robot's decisions are based on self-learning processes, the causality between human action and technical result can break down. Without complete protocols, the culpability principle becomes empty. De lege ferenda, a duty of technical traceability should therefore be introduced. Audit trails, real-time protocols and independent testing procedures are not only medically, but dogmatically indispensable because they keep action, causality and guilt provable (Issa 2025; Pane & Permana 2025; Zamani 2025).

4.3 Autonomous weapon systems

In the military context, international humanitarian law applies de lege lata. Art. 36 CP I obliges states to check new weapons systems for compatibility with international law before they are deployed. However, without verifiable control structures, it is almost impossible to determine whether an attack is the result of a human order or a machine error. The debate about Meaningful Human Control is therefore not a political platitude, but a dogmatic necessity. It forms the bridge over which the principle of guilt can be maintained in digital warfare.

In the Schrems I (2015) and Schrems II (2020) judgements, the European Court of Justice emphasised that technical systems must be measured against fundamental rights standards. Even if these decisions are not aimed at weapons law, they transfer the principle of fundamental rights to algorithmic control. It follows from this: Lethal decisions without human control violate Art. 1 GG, Art. 2 ECHR and fundamental principles of international criminal law (Samakashvili 2025).

4.4 Cross-cutting findings

Firstly, responsibility shifts from the intervention phase to upstream stages of design, training and organisation. De lege lata, negligence offences and organisational duties already apply, but their scope remains limited if they cannot be proven. Secondly, individual culpability and organisational responsibility complement each other. Managers are liable if they do not clearly define or monitor the scope of their duties.

Thirdly, fictions of artificial culpability have no dogmatic basis. Attribution must remain tied to real decision-makers who can act,

influence causality and bear guilt. Fourthly, without preventive obligations to auditability, criminal law loses its enforceability. Only traceable data chains make the elements of an offence practically applicable. Fifthly, the comparison shows that criminal law operates on several levels: nationally through the principle of guilt and due diligence, at European level through documentation obligations and under international law through human rights standards.

4.5 Consequences for the research question

The case analyses confirm that criminal imputability remains possible even in the age of autonomous systems if it is anchored in new norms. De lege lata, negligence offences and organisational duties are effective, but they do not completely close the responsibility gap. De lege ferenda, catalogues of obligations, auditability and international standards must be explicitly codified so that accountability does not become a black box effect. Attributability thus becomes a design principle of technical systems: criminal law remains capable of acting if it visibly assigns responsibility, enforces transparency and preserves human dignity as an inviolable boundary.

5 Legal and Ethical Challenges

Autonomous systems pose not only dogmatic but also normative and political challenges for criminal law. The classic logic of attribution is based on personal guilt, individual responsibility and verifiable causality. These cornerstones are shaken when decisions are influenced or completely generated by learning systems. Criminal attribution must therefore examine how the principle of guilt, verifiability and human dignity can be preserved under the conditions of technical autonomy.

5.1 Dogmatics and the principle of culpability

De lege lata, the principle of guilt remains unshakeable. Criminal liability presupposes personal culpability. Action, intent, negligence and guilt must be attributed to a natural person (Sections 13, 14 StGB). Machines are not legal subjects; they cannot commit an act, form an intention or recognise wrongdoing. The idea of electronic perpetration is dogmatically untenable (Cuccuru 2025; Globke 2021). However, responsibility can be imparted through breaches of duty. Programmers, manufacturers, operators or users are criminally liable if they violate testing, monitoring or update obligations. These breaches concretise the objective duties of care on which negligence offences are based. De lege ferenda, criminal law should explicitly standardise these duties in order to create dogmatic consistency without abandoning the principle of culpability. This would create a binding link between individual and structural responsibility.

5.2 Transparency and verifiability

Criminal law can only be applied if facts can be proven. Non-transparent or self-learning systems jeopardise this principle because they make it difficult to prove actions, causality and guilt. In the absence of logs or audit trails, evidence becomes uncertain. Judgements in medical and traffic law show that courts are dependent on complete documentation. The AI Act and the Product Liability Directive 2024 already stipulate documentation and inspection obligations, which could also become a criminal offence in the future. A legal obligation to auditability should therefore be enshrined in the future. Logs, real-time protocols and independent audit procedures should be mandatory. Failure to do so will result in a criminal offence because it will be impossible to provide evidence in criminal proceedings (Sommer 2020; Armbrüster 2020; Issa 2025).

Criminal procedural law is also gaining new significance. Art. 6 ECHR guarantees a fair trial and the right to an effective defence. If algorithms are used as evidence, their functionality must be verifiable. Without disclosure of the system logic, asymmetrical

proceedings arise that undermine the principle of guilt. Transparency obligations are therefore necessary both in substantive and procedural terms.

5.3 Human dignity and legitimacy

De lege lata, Article 1 of the Basic Law protects human dignity as the highest standard for all state action. Decisions on life or death without human control violate this principle, as do Art. 2 ECHR and international humanitarian law. Systems that make irreversible decisions without the possibility of human intervention are contrary to the rule of law.

De lege ferenda, these guidelines should be explicitly codified. Three points are central:

- Meaningful human control in the military sector as a binding standard,
- Duty of disclosure in the medical context to ensure informed consent,
- fairness and traceability standards for algorithmic procedures in the judiciary and administration.

Hildebrandt (2016) and Khazaei & Hemmati (2025) emphasise that these human rights guard rails are not just ethical postulates, but legal dogmatic prerequisites. Attribution only remains legitimate if it is based on a conception of humanity that recognises responsibility, guilt and the protection of dignity as inseparable.

5.4 Ethics of responsibility and the political dimension

Criminal law cannot be separated from ethical responsibility. It intervenes as ultima ratio when moral, technical and organisational control fails. Autonomous systems shift this threshold because algorithmic decisions diffuse responsibility.

Attribution must therefore also be redefined in terms of the ethics of responsibility. Responsibility arises where developers, supervisory authorities, medical practitioners, military planners and political decision-makers have the power to organise. This responsibility is structural, but concrete: it requires active assurance of transparency, fairness and control. Criminal law is ethically reactive, but normatively guiding. It defines what society understands by legitimate responsibility.

5.5 Interim conclusion

The legal and ethical challenges of autonomous systems are centred on three core elements: the principle of culpability, verifiability and human dignity. Firstly, the principle of culpability as the main pillar of criminal law is under pressure to adapt, but must not be abandoned. Attribution to natural persons must remain tied to those who have the power to organise and the duty to supervise. Secondly, the enforceability of criminal law depends directly on transparency and auditability. Without traceable data chains, audit trails and control mechanisms, the elements of the offence lose their practical applicability.

Thirdly, human dignity is the absolute limit of criminal law legitimacy. Systems that decide on life, liberty or sentencing without human control violate fundamental principles of the Basic Law and the ECHR. Ensuring Meaningful Human Control is therefore not an ethical recommendation, but a legal obligation.

Together, these three elements show that criminal law and ethics are only capable of acting together. The principle of guilt gives responsibility normative depth, transparency makes it provable, and human dignity limits it under the rule of law. In this interplay, criminal attribution can also endure in a world of technical autonomy.

6 International perspectives

Autonomous systems are not a national phenomenon. They operate in transnational infrastructures, global supply chains and normative grey areas. Criminal attribution is therefore challenged on several levels, reflecting different legal cultures and value systems. Three basic lines can be recognised: The principle of guilt dominates in democratic constitutional states, preventive regulation in the European Union and a political instrumentalisation of responsibility in authoritarian systems.

6.1 German criminal law

German criminal law remains dogmatically based on the principle of culpability. Action, intent, negligence and culpability form the standard for all attribution. This structure also applies to autonomous systems, but comes up against technical and epistemic limits when machine processes interrupt the chain of action. Nevertheless, there are viable connecting factors: § Section 13 StGB enables attribution via guarantor duties, Section 14 StGB via representation facts, Sections 30, 130 OWiG via organisational duties. They form the backbone of a personal responsibility logic, even in the case of technical mediation. De lege ferenda, this system should be supplemented by specific obligations regarding auditability, data validation and update governance in order to ensure verifiability and the principle of culpability.

6.2 European Union

The European Union pursues preventive, risk-based regulation. The AI Act creates transparency, documentation and security requirements for high-risk systems. Although these requirements are based on administrative and civil law, they have an indirect effect on criminal law because they define the standards of dutiful behaviour. The Charter of Fundamental Rights (Art. 1, 7, 8) forms the normative framework. It guarantees human dignity, privacy and data protection rights, which are also decisive in the interpretation of due diligence obligations under criminal law. A breach of documentation obligations can therefore not only have consequences under civil law, but also under criminal law in cases of gross negligence. De lege ferenda, the EU should explicitly establish this link. Codifying obligations relevant to criminal law would strengthen the protection of fundamental rights and link attribution to preventive structures. Europe could thus develop a multi-level system that combines prevention and legitimacy.

6.3 United States

The United States pursues a governance-oriented approach. Criminal law takes a back seat, while liability is regulated by civil law and internal corporate mechanisms. The State v. Loomis judgement (2016) accepted algorithmic risk predictions despite their non-transparent functioning, blurring the line between individual culpability and statistical probability. In civil law, the Caremark doctrine obliges company management to set up effective control systems for material risks. Violations lead to civil, not criminal, liability. Responsibility is thus functionally distributed, but not normatively anchored. This efficiency logic protects markets, not human dignity. The lesson for Europe is that prevention without a normative commitment leads to regulatory emptiness.

6.4 Authoritarian systems

In authoritarian legal systems, the principle of guilt takes a back seat. Autonomous technologies serve there as a means of social control. Responsibility is distributed according to state opportunity, not according to individual blameworthiness. Misbehaviour of technical systems is not seen as a legal problem, but as a need for political adaptation. This breaks the link between action, guilt and legitimacy in a development that also puts international standards under pressure.

6.5 Global fault lines and integration perspective

An international comparison reveals three patterns:

- Germany adheres to personal guilt and guarantor duty.
- The European Union is developing a preventive-regulatory system.
- The United States externalises responsibility in governance mechanisms, while authoritarian systems politicise it.

De lege ferenda, this gives rise to a twofold task. Firstly, constitutional democracies must establish common minimum standards for transparency, auditability and human

control. Secondly, criminal law must preserve its normative identity by maintaining the principle of guilt and human dignity as universal points of reference. Criminal attribution thus becomes a question of global legal culture. It determines not only liability, but also the understanding of responsibility in a technologised world. Only if states base their standards on common principles will law remain an instrument of freedom and not of control.

7 Future Prospects and Proposed Solutions

Autonomous systems force a readjustment of criminal law. The classic elements of offence, causality, intent, negligence and guilt remain the foundation, but are no longer sufficient to close gaps in responsibility. The future of criminal law will depend on whether it can combine its personal categories with preventive and organisational duties without relativising the principle of culpability.

7.1 National level

German criminal law has sound foundations. Negligence offences and guarantor duties offer starting points for assigning responsibility to people who design or use technical systems. Regulatory offence law also allows sanctions to be imposed on companies if managers violate their supervisory duties.

However, these standards are only partially effective. The complexity of learning systems requires specific due diligence standards. De lege ferenda, a binding catalogue of obligations should therefore be created that includes auditability, data quality, update governance and incident response processes. In addition, there is a need for corporate criminal law that makes organisations liable for structural breaches of duty. Such a model strengthens accountability because it anchors responsibility where decisions about risk and control are actually made. At the same time, it upholds the principle of culpability by systematically linking individual and organisational responsibility.

7.2 European level

At European level, the AI Act is already creating a framework of preventive responsibility. In future, these standards must be made compatible with criminal law. Breaches of documentation, auditing or transparency obligations should not only have consequences under civil or administrative law, but also under criminal law. The European Union can thus take on a pioneering role. If it explicitly codifies obligations relating to auditability, data integrity and human control as standards that can be reviewed under criminal law, a model of regulatory attribution is created. It combines prevention, protection of fundamental rights and legitimacy and provides a counterbalance to purely economic governance approaches. In addition, the EU should push ahead with harmonisation. Minimum standards for criminal liability in high-risk AI systems increase legal certainty and prevent companies from exploiting differences between Member States. Coherence in criminal law thus becomes a factor of European stability.

7.3 International level

A binding legal framework is still lacking on a global scale. International humanitarian law does contain an obligation to test new weapons technologies in Article 36 of ICP I, but this norm can only be applied to civilian AI applications to a limited extent. De lege ferenda, an international minimum standard should be developed that comprises three elements:

- An obligation for traceability and preservation of evidence for safety-critical autonomous systems,
- a codification of human control obligations for lethal applications,
- an obligation to report on risk assessments and system validations.

These standards could be implemented in the form of an additional convention to existing

human rights treaties or a multilateral agreement. Due to its normative orientation, the European Union would be predestined to take on a leading role. Only international coordination can prevent technical efficiency from becoming the yardstick of legal legitimacy.

7.4 Ethical guard rails

The further development of criminal law must not be technocratic. It must be based on a clear conception of humanity. Article 1 of the Basic Law and Article 2 of the ECHR form the basis of any legitimate liability model. De lege ferenda, human dignity should therefore be explicitly operationalised in technology-specific laws. These include

- the prohibition of fully autonomous lethal decisions without human control,
- information obligations and consent in the medical field,
- fairness and traceability standards for algorithmic decisions in the justice system.

Ethics and dogmatics are not mutually exclusive. The ethical dimension lends legitimacy to the law, while dogmatic precision makes it verifiable.

7.5 Synthesis

The criminal law of the future will only remain capable of acting if it combines responsibility, transparency and human dignity into a coherent system. De lege lata, there are viable starting points in the form of negligence offences, organisational duties and regulatory offences. De lege ferenda, this structure must be expanded to include preventive control mechanisms and international standards.

In future, responsibility will not only be determined retrospectively, but also prospectively. The obligation to recognise, document and control risks forms the core of criminal law legitimisation. This will transform criminal law from a reactive to a formative system. It remains the guarantor of human freedom in a world in which technical systems increasingly influence decisions.

8 DISCUSSIONS

The analysis makes it clear that criminal law remains capable of acting even in the age of autonomous systems if it preserves its normative foundations and at the same time adapts to the requirements of technical development. Responsibility, transparency and human dignity form a coherent structure that guarantees the legitimacy of criminal attribution.

8.1 Preserving the principle of culpability

The principle of guilt remains the central criterion of criminal law legitimisation. Machines cannot be perpetrators, which is why imputation must continue to be linked to persons who have the power to organise and control. Sections 13 and 14 StGB provide viable structures for this. De lege ferenda, this logic should be supplemented by codified catalogues of obligations that create clear standards for monitoring, data validation and auditability. Humans remain the subject of the law, even when machines act. Their normative responsibility cannot be delegated. Any technical mediation must be balanced by legal control obligations so that criminal law retains its accountability in complex systems.

8.2 Interweaving of dogmatics and regulation

National, European and international levels form a normative cascade. At national level, negligence offences and guarantor duties ensure individual responsibility. At European level, the AI Act establishes preventive control mechanisms. In the international context, Art. 36 of the first article of the ICC and human rights minimum standards guarantee protection against structural irresponsibility. This interplay leads to a new logic of criminal law. Responsibility is no longer determined exclusively retrospectively, but is structured preventively. Criminal law is developing from a reactive to a formative system that balances freedom of action and the rule of law.

8.3 Limits and risks

Despite these prospects, there are considerable challenges. Firstly, the technical intransparency of many AI systems jeopardises the ability to prove causality and guilt. Secondly, there is a risk of normative overextension if responsibility is shifted to organisational processes without ensuring individual accountability. Thirdly, a fragmentation of international standards can create new legal uncertainties. These limits show that dogmatics, politics and technology remain interdependent. Criminal law can demand transparency, but it cannot create it alone. It needs co-operation with technology, ethics and governance to ensure its ability to function.

8.4 Legitimisation in the digital age

In future, the legitimisation of criminal attribution will be based on three conditions. Firstly, decision-making processes must be comprehensible. Secondly, obligations must be verifiable. Thirdly, human dignity must remain inviolable. Only in this combination can criminal law retain normative authority. The law does not have to put the brakes on technical innovation, but it must not limit responsibility. Criminal law norms should protect room for manoeuvre, not conceal shifts in power. The aim remains to secure freedom through responsibility and to prevent control through technology.

8.5 Concluding thoughts

This study confirms that imputability is not a relic of anthropocentric dogmatism, but an expression of the modern rule of law. The criminal law of the future will be measured by whether it makes responsibility visible without suppressing autonomy. If it guarantees transparency, creates normative clarity and preserves human dignity as the limit of technical agency, it will remain the most effective instrument of rational freedom in a world of autonomous systems.

9 LIMITATIONS

This study has shown that autonomous systems challenge the dogmatic structure of criminal law. At the same time, it can be recognised that any analysis remains bound by methodological and normative limits. The work concentrates on the dogmatic and systematic level. Empirical reviews of actual liability cases or court decisions are not yet available to a sufficient extent. Firstly, there is a substantive limitation due to the rapid pace of technological development. New forms of machine autonomy may change the assumptions formulated here in the future. Legislation and case law react with a time lag, which means that normative concepts in dynamic fields can quickly become outdated. Secondly, the comparability of international regulations is limited. Legal systems differ in terms of structure, values and dogmatics. The comparison of democratic, European, US-American and authoritarian systems undertaken here can therefore only be understood as an example. Thirdly, the transferability of the proposed catalogues of obligations remains theoretical. Their practical implementation depends on political decisions, institutional capacities and technical traceability. This is particularly true for international standards, which remain difficult to enforce without binding mechanisms. Fourthly, the study can only address the problem of evidence dogmatically. The question of whether machine decisions can actually be retraced in criminal proceedings cannot yet be empirically tested.

As long as technical transparency and auditability are not reliably ensured, the implementation of the proposed models remains uncertain.

Ultimately, the proposed solutions are normative drafts. They describe conceivable developments, not applicable law. The proposal to concretise responsibility via organisational duties and auditability is aimed at the further development of criminal law, not at immediate reform. The limitations of this work therefore lie in its dependence on technical and political developments and the lack of empirical verification of the dogmatic concepts. Nevertheless, the results obtained form a sound basis for future

research that can more closely combine legal theory, technology law and empirical legal analysis.

10 CONCLUSIONS

The study has shown that autonomous systems pose a fundamental challenge to criminal law. Where technical processes influence decisions, gaps in responsibility arise that classical categories can only close to a limited extent. Nevertheless, criminal law remains capable of acting if it preserves its dogmatic structures and at the same time develops new normative instruments. Attributability is still possible as long as it remains related to the acting persons who are responsible for the planning, deployment and control of autonomous systems. The principle of culpability, enshrined in Sections 13 and 14 of the German Criminal Code, forms the core of this legitimisation. It ensures that only the person remains the bearer of criminal responsibility. The work has shown that auditability, organisational obligations and verifiability are key prerequisites for modern attribution. Without traceable data chains, audit trails and control mechanisms, criminal law loses its enforceability. Preventive structures must therefore be an integral part of criminal law dogmatics in the future.

At European level, the AI Act and the Product Liability Directive 2024 form the starting point for preventive regulated responsibility. These instruments create standards for dutiful behaviour that can be integrated into national criminal law. Internationally, Art. 36 ZP I and human rights standards supplement the protective framework by ensuring transparency, human control and provability in normative terms. The relationship between technology, ethics and law requires a new balance. Criminal law must not hinder innovation, but must retain its normative integrative power. It has the task of making responsibility visible, protecting freedom and binding state control to human dignity.

The future of criminal law lies in its ability to curb technical power without hindering social development. If we succeed in combining responsibility, transparency and human dignity into a consistent system, criminal law will remain the guarantor of human freedom and rational order even in the age of autonomous systems.

Declaration by Author

Acknowledgement: None
Source of Funding: None
Conflict of Interest: No conflicts of interest declared.

About the Author

Enrico Moch holds a doctorate in economics and a master's degree in law. He teaches as a lecturer at various universities, including DHBW Ravensburg, and as an assistant professor at the IIC University of Technology. As Academic Director of the GrandEdu Research School in Germany, he combines academic excellence with practice-oriented teaching. His research interests include the Austrian School of Economics, AI governance, technical data protection, and the institutional governance of digital platforms. Dr Moch publishes regularly in academic journals, contributes to interdisciplinary book projects, and hosts the podcast "GrandEdu Research School - On the Trail of the Economy." He is also actively engaged in academic peer review and is committed to bridging research and practice to promote long-term understanding of economic and social development issues.
https://orcid.org/0009-0005-4722-0961

11. REFERENCES

1. Armbrüster, C., & Thöne, M. (2020). Autonomous systems and tortious liability. Journal for the entire science of insurance, 109(2), 137-141. https://doi.org/10.1007/s12297-020-00472-y
2. Bryson, J. J. (2018). Patience is not a virtue: The design of intelligent systems and

systems of ethics. Ethics and Information Technology, 20(1), 15-26. https://doi.org/10.1007/s10676-018-9448-6

3. Cuccuru, C. (2025). Intelligenza artificiale e responsabilità penale [Doctoral dissertation, Università degli Studi di Sassari]. Università degli Studi di Sassari. https://tesidottorato.depositolegale.it/bitstream/20.500.14242/210082/1/INTELLIGENZA%20ARTIFICIALE%20E%20RESPONSABILITA%3F%20PENALE.pdf
4. Daly, A., Hagendorff, T., Hui, L., Mann, M., Marda, V., Wagner, B., ... Witteborn, S. (2019). Artificial Intelligence Governance and Ethics: Global Perspectives. arXiv. https://arxiv.org/abs/1907.03848
5. Essers, D. (2024). Liability issues of automated systems. Duncker & Humblot.
6. Feldmann, J. (2024). Autonomous vehicles and criminal law issues. MANZ. https://doi.org/10.5771/9783214258917
7. Globke, C. (2021). Promises of autonomy. Franz Steiner Verlag. https://www.steiner-verlag.de/Verheissungen-der-Autonomie/9783515129305
8. Gruber, M.-C., Bung, J., & Ziemann, S. (2015). Autonomous automata: Artificial bodies and artificial agents in a technologised society. BiblioScout. https://doi.org/10.35998/9783830520566
9. Grützmacher, M. (2016). Tort liability for autonomous systems -Industry 4.0 as a challenge for existing law? Computers and Law, 32(10), 695-698. https://doi.org/10.9785/cr-2016-1015
10. Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. Minds and Machines, 30, 99-120. https://doi.org/10.1007/s11023-020-09517-8
11. Helm, P., & Gerlek, S. (2025). Empirical AI Ethics: Reconfiguring Ethics towards a Situated, Plural, and Transformative Approach. arXiv. https://arxiv.org/abs/2509.17727
12. Hildebrandt, M. (2016). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.
13. Hilgendorf, E. (2018). Dilemma problems in automated driving: A contribution to the problem of the prohibition of offsetting in the age of digitalisation. Zeitschrift für die gesamte Strafrechtswissenschaft, 130(3), 674-703. https://doi.org/10.1515/zstw-2018-0027
14. Issa, H. B. (2025). Robotic surgery and the law: Defining control and criminal responsibility. Journal of Soft Computing and Data Mining. https://publisher.uthm.edu.my/ojs/index.php/jscdm/article/view/22143/7373
15. Yeung, K. (2019). Responsibility and AI: Council of Europe Study DGI(2019)05. Council of Europe. https://rm.coe.int/responsability-and-ai-en/168097d9c5
16. Khazaei, H., & Hemmati, M. (2025). Assessment of AI conflict with human rights. Modern Technologies Law Journal. https://mtlj.usc.ac.ir/article_212704_ca55fc66fd1f201704aad93e47b60a73.pdf
17. Körber, T., & Koenig, C. (2020). Liability Law 4.0. In Handbook Industry 4.0 (pp. 233-246). Springer. https://doi.org/10.1007/978-3-662-58474-3_14
18. Moafa, F. A., & Almarri, H. S. (2025). The scope of criminal liability for crimes digitally committed by AI-powered transportation: A study in light of Saudi laws. Lex Localis. https://lex-localis.org/index.php/LexLocalis/article/view/800686/1441
19. Moraiti, A. (2025). Artificial intelligence and the general part of criminal law: Paradigm shifts of criminal accountability and imputation. University of Luxembourg. https://orbilu.uni.lu/handle/10993/64975
20. Münster, M. (2022). Punished innovation? Duncker & Humblot. https://www.duncker-humblot.de/_files_media/leseproben/9783428584352.pdf
21. Pane, M. D., & Permana, M. Z. S. (2025). Pertanggungjawaban pidana terhadap pengembang AI. Judge: Jurnal Hukum. http://journal.cattleyadf.org/index.php/Judge/article/download/1593/879
22. Samakashvili, A. (2025). Code, command, and consequences: Who is responsible for war crimes committed by lethal autonomous weapon systems (LAWS)? Air and Space Law Journal. https://jrnl.nau.edu.ua/index.php/UV/article/view/20212/27313
23. Sommer, M. (2020). Liability for autonomous systems. Nomos. https://doi.org/10.5771/9783748921943-1
24. Zamani, M. (2025). Algorithms, automation and accountability: Imagining responsibility for the crimes of machines. SSRN.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5405090

Judgements

1. Federal Court of Justice. (15 June 2010). Judgement, Ref. VI ZR 204/09 (published in NJW 2010, 3330).
2. Federal Court of Justice. (1979). BGHSt 29, 317 - Pacemaker case.
3. European Court of Justice. (6 October 2015). Maximillian Schrems v Data Protection Commissioner, Case C-362/14.
4. European Court of Justice. (16 July 2020). Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18.
5. In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996). https://law.justia.com/cases/delaware/court-of-chancery/1996/13670-3.html
6. Darmstadt Regional Court. (21 February 2022). Judg. v. 21 February 2022, file number 26 O 490/20.
7. Regional Court Munich I. (17 June 2022). Judgement of 17 June 2022. 17 June 2022, case no. 4 O 3834/19.

How to cite this article: Enrico Moch. Autonomous systems (AI) and criminal imputability: challenges for modern law. *International Journal of Research and Review*. 2025; 12(10): 287-301. DOI: *https://doi.org/10.52403/ijrr.20251029*

******