CRIMINAL LIABILITY MODELS AND CRIMINAL PARTICIPATION IN THE DIGITAL ENVIRONMENT: A MODERN CHALLENGE IN THE PERSPECTIVE OF ITALIAN CONSTITUTIONALISM

Abstract: The rapid progression and widespread integration of Information and Communication Technology (ICT) have ushered in a new era of sweeping social and legal transformations. Among the many groundbreaking advancements, Artificial Intelligence has emerged as a pivotal force, permeating nearly every facet of our daily lives. From the realms of commerce and industry to healthcare, transportation, and entertainment, Artificial Intelligence technologies have become indispensable tools shaping the way we interact, work, and navigate the world around us. With its remarkable capabilities and ever-expanding reach, Artificial intelligence stands as a testament to humanity’s relentless pursuit of innovation and the boundless potential of technology to revolutionize society. While completing all the tasks they are programmed for, Artificial Intelligence systems can perform actions, which could result in crimes if committed by humans. But crimes follow the reserve of law, therefore can be difficult to criminalize such crimes because of the lack of written law. Nevertheless, in modern legal systems, the structure of crimes doesn’t only require the commission of a typical fact, but also the determination to do it.

In this scenario, being Artificial Intelligence a non-human entity, the reconstruction of criminal responsibility is particularly difficult to theorize. This is mainly true because of the peculiar nature of the environment the machine lives in: the digital environment is made of a digital reality, and many of its actors (for example algorithms, protocols, and programs) are not even human and can only exist in that reality. This means that in this environment, machines can act, determine themselves and possibly commit crimes with or without a human user.
This scenario makes it necessary to analyze Artificial Intelligence crimes in the light of common ones, using the ordinary law discipline. This analysis allows users (lawyers, judges, and scholars) to use three traditional liability models: “the perpetration-via-another”, “the natural probable consequence”, and “the direct liability”. Through these models, users can assess whether the machine committed a crime.

Nevertheless, the three liability models supra mentioned open the door to a totally modern scenario: the man-machine concurrence (the concurrence between man and Artificial Intelligence algorithm). In fact, if theorizing the liability of the machine comes with challenges, it is even more complicated to adapt to modern Constitutions the concurrence between the living and the digital. Indeed, it is necessary to assess whether a machine can commit crimes (or it is just an instrument), determine how the machine can concur with a human, and how much responsibility can be addressed to it.

This paper wants to analyze the peculiarities of Artificial Intelligence, deconstruct three possible Artificial Intelligence liability models, and, finally, theorize the criminal participation man-machine through the lenses of Italian law.

**Keywords**: Liability, actus reus, participation, programmer, algorithm, criminal law.

### 1. INTRODUCTION

In 2023, Artificial Intelligence (AI) is a dominant and pervasive force, driven by swiftly adaptable techniques, including machine learning algorithms, data mining, and predictive systems. These techniques portend an extraordinary – and perhaps somewhat disconcerting – level of Artificial Intelligence integration into our lives and societies. Currently, these techniques find applications in most sectors: from internet browsers and smartphone applications to video games, from engineering projects and animated graphics to hospitals and research.

---

The notion of Artificial Intelligence’s substantial presence extends further, with luminaries like Stephen Hawking foreseeing a future where computer intelligence surpasses human capabilities within a century\textsuperscript{4}.

The 2017 European Parliament’s Resolution on robotics similarly hints at the potential for Artificial Intelligence to transcend human intellectual prowess. This omnipresence of Artificial Intelligence necessitates a legal response\textsuperscript{5}. It compels criminal law, in particular, to brace itself for a technological revolution akin to historical transitions and grapple with challenges that this transformation may pose\textsuperscript{6}. Addressing this requires assessing the adaptability of existing norms to accommodate novel technologies, deliberating on the appropriateness of formulating new, tailored regulations, or, alternatively, persevering with existing laws, albeit with potential strains, possibly with the backing of precedent law\textsuperscript{7}.

This endeavor must be imbued with a focus on harmonizing these legal developments with fundamental rights such as due process, privacy, and equality\textsuperscript{8}.


\textsuperscript{5} As already highlighted in C. Piparo, *Ibid.: “The European Parliament Resolution of 16 February 2017, providing recommendations to the European Commission on civil law rules on robotics (2015/2103(INL)), is a document that offers guidance and suggestions to the European Commission regarding the need to develop specific civil law rules for the field of robotics. The document represents a significant step in addressing the legal and social implications associated with the advancement of robotic technology.

The Resolution highlights the importance of creating a clear and consistent legal framework that addresses issues related to liability and safety in the field of robotics. It recognizes that the increasing presence of robots and artificial intelligence poses a range of challenges, including determining responsibility in case of damages caused by a robot, protecting personal data, and ensuring the safety of the robots themselves.

Through this Resolution, the European Parliament calls upon the European Commission to consider the adoption of a specific legal framework for robotics that takes into account ethical principles and the fundamental rights of individuals. It also emphasizes the need to promote research and innovation in the field of robotics to ensure that Europe remains competitive in this rapidly evolving sector.

In summary, the European Parliament Resolution of 16 February 2017 is an important document that raises the issue of civil law rules on robotics and urges the European Commission to consider this challenge and take appropriate measures to address it”.

\textsuperscript{6} C. Piparo, *Machina delinquere potest?*, cit., p. 901.

\textsuperscript{7} Federico Stella, *Giustizia e modernità. La protezione dell’innocente e la tutela delle vittime*, 2003, pp. 292 seq.

2. THE CONCEPT OF ARTIFICIAL INTELLIGENCE

Today, the use of the expression Artificial Intelligence\(^9\) assumes various connotations and interpretations contingent on the specific discipline or context of reference\(^10\), thus leaving no \textit{passe partout} definitions.

Approximately three decades later, in a 1987 essay, Roger Schank, a prominent Artificial Intelligence theorist and a foundational figure in computational linguistics, ascribed five attributes to AI: the capacity for communication, self-awareness, understanding of external reality, purposive action driven by goals, and a notable degree of creativity, which encompasses the ability to make alternate decisions when the initial course of action proves unsuccessful or unfeasible\(^11\). This set of features offers two key insights: firstly, Artificial Intelligence can’t be confined to the realm of intelligent humanoid figures or cyborgs; at most, the latter can manifest as an Artificial Intelligence application. Secondly, Artificial Intelligence systems cannot replicate the cognitive mechanisms of the human mind.

Consequently, it is more apt to regard Artificial Intelligence as a computational discipline rather than an emulation of the intricate human biological system\(^12\). Experts in Artificial Intelligence tend to prefer the term “rationality\(^{13}\)” over

---

\(^9\) The epithet Artificial Intelligence was coined by American computer scientist John McCarthy in 1955. See also C. Piparo, \textit{Machina delinquere potest?}, cit., where the Author states that “The term is publicly used by the scholar during a seminar held at Dartmouth College. The scholar continued his studies in the field of artificial intelligence, which led him to win the Turing Award in 1971 for his significant contributions in this area”.

\(^10\) To learn more, see also Carlos Ignacio Gutierrez, Anthony Aguirre, Risto Uulk, Claire Boine, Matija Franklin, \textit{A Proposal for a Definition of General Purpose Artificial Intelligence Systems}, 2022, where the Author states that: “As it stands today, no guidelines explain the inclusion criteria for AI systems that classify as General Purpose Artificial Intelligence Systems (GPAIS). Within the AI Act context, the existing definition has many opportunities for improvement. The Slovenian EU presidency defined GPAIS as an “AI system... able to perform generally applicable functions such as image/speech recognition, audio/video generation, pattern detection, question answering, translation, etc”. The French EU presidency further emphasizes that GPAIS: “may be used in a plurality of contexts and be integrated in a plurality of other AI systems”. Outside the EU context, the term GPAIS is seldomly and haphazardly used to describe AI systems that vary considerably in terms of autonomy, agency, modality, and training methods”.


\(^12\) J. Kaplan, \textit{Intelligenza artificiale}, cit., p. 41.

\(^13\) In Stuart Russel, Peter Norvig, \textit{Artificial Intelligence: A Modern Approach}, Prentice Hall, 3rd edition, 2009, pp. 36 seq., the Authors discuss about the concept of “rational agent”, defining it as is the agent that consistently makes choices that maximize its expected performance, given its percept sequence (historical sensory input), the performance measure (a criterion for success), and any built-in knowledge about its environment. In essence, rationality means selecting actions that are likely to lead to the best overall outcomes, considering the information available to the agent up to that point.

According to the Authors, rationality does not require omniscience; instead, it operates based on the agent’s perception of the world and its past experiences. It encompasses the ability to
“intelligence”, denoting the ability to select the most optimal path to achieve specific aims, guided by criteria for resource optimization. As already stated “other definitions go further in explaining [...] skills and tasks. For example, the computer scientist Nils John Nilsson describes a technology that “functions appropriately and with foresight in its environment”. Others speak of the ability to perceive, to pursue goals, to initiate actions and to learn from a feedback loop.

A similar definition has been put forward by the High-Level Expert Group on Artificial Intelligence (AI HLEG) of the European Commission (EC): “Systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals”.

These task-based definitions go some way towards giving us a better understanding of what AI is. But they still have limitations. Concepts like “some degree of autonomy” remain somewhat vague. Moreover, these definitions still seem overly broad in that they describe phenomena that most of us would not be inclined to bundle under the term AI. For example, Nilsson’s definition also applies to a classic thermostat. This device is also able to perceive (measure the temperature of the room), pursue goals (the programmed temperature), initiate actions (regulate the thermostat) and learn from a feedback loop (stop once the programmed temperature has been reached). Even so, most people would not be inclined to regard a thermostat as AI.

The European Ethical Charter, adopted by the European Commission for the Efficiency of Justice in 2018, frames Artificial Intelligence as “the set of scientific methods, theories, and techniques aimed at reproducing through machines gather information, explore unknown environments, and adapt behavior based on learning from these experiences. Rational agents are autonomous in the sense that they can make decisions independent of complete prior knowledge, relying on their perception and past learning to make informed choices. In summary, rationality, as defined in the paper, represents a fundamental principle in artificial intelligence, guiding agents to make decisions that optimize their performance based on the information available to them and their understanding of the environment.

Within Europe, the acronym CEPEJ signifies the European Commission for the Advancement of Justice Efficiency. Originating as an entity operating under the Council of Europe’s umbrella, CEPEJ stands dedicated to the continual enhancement of justice systems within the member states it encompasses. Its inception was driven by the mission to foster greater accessibility to justice, elevate the standard of judicial services, and uphold the principles of fairness in legal proceedings.

A fundamental facet of CEPEJ’s role revolves around the development and implementation of standardized tools, methodologies, and benchmarks. These elements serve as catalysts for the progressive transformation of justice systems throughout Europe. CEPEJ offers its expertise, offering valuable guidance to member states, delving into comprehensive research endeavors, and amassing invaluable data to evaluate the functionality of judicial systems. Through these multifaceted efforts, CEPEJ aims to discern and promote best practices, stimulate collaborative research and policy development, and ultimately contribute to the transformation of justice systems across Europe.

16 Within Europe, the acronym CEPEJ signifies the European Commission for the Advancement of Justice Efficiency. Originating as an entity operating under the Council of Europe’s umbrella, CEPEJ stands dedicated to the continual enhancement of justice systems within the member states it encompasses. Its inception was driven by the mission to foster greater accessibility to justice, elevate the standard of judicial services, and uphold the principles of fairness in legal proceedings.

A fundamental facet of CEPEJ’s role revolves around the development and implementation of standardized tools, methodologies, and benchmarks. These elements serve as catalysts for the progressive transformation of justice systems throughout Europe. CEPEJ offers its expertise, offering valuable guidance to member states, delving into comprehensive research endeavors, and amassing invaluable data to evaluate the functionality of judicial systems. Through these multifaceted efforts, CEPEJ aims to discern and promote best practices, stimulate collaborative
the cognitive abilities of human beings”. It emphasizes the present aim of delegating complex tasks previously performed by humans to machines. In contrast, the European Commission’s 2018 Communication on Artificial Intelligence in Europe characterizes Artificial Intelligence as “systems that exhibit intelligent behavior by analyzing their environment and autonomously taking actions to achieve specific goals”. This definition encompasses Artificial Intelligence systems in both the virtual realm, such as voice assistants, image analysis software, and search engines, and those integrated into physical hardware, including advanced robots, self-driving vehicles, drones, and Internet of Things applications. A scrupulous examination by the Independent High-Level Expert Group, appointed by the European Commission for advisory purposes on Artificial Intelligence, aligns with the foregoing definitions. According to this group, the concept of Artificial Intelligence denotes “human-designed software (and potentially hardware) that, when presented with a complex goal, operates in the physical or digital realm by perceiving its environment through data acquisition, interpreting structured or unstructured data, reasoning based on knowledge or information derived from these data, and determining the optimal course of action to attain the specified goal”. AI systems can adopt symbolic rules or acquire a numerical model, and they are also capable of adapting their behavior by analyzing the consequences of their prior actions on the environment. As a scientific discipline, AI encompasses a gamut of approaches and techniques, including machine learning, mechanical reasoning, and robotics, integrating various methods within cyber-physical systems. Consequently, while the scientific community employs diverse definitions of Artificial Intelligence, certain common characteristics emerge. In summation, Artificial Intelligence generally alludes to a compendium of scientific methodologies, theories, and techniques with the objective of replicating human cognitive abilities through mechanized means.

CEPEJ’s mandate extends across various dimensions of judicial efficiency. It encompasses areas such as case management, judicial administration, adherence to legal timelines, the quality of legal pronouncements, and the integration of cutting-edge information technologies into the realm of justice. Furthermore, CEPEJ delves into issues pertaining to the accessibility of justice, judicial training programs, and the critical evaluation of existing judicial systems.

By advocating for core principles, namely efficiency, accessibility, and impartiality in the administration of justice, CEPEJ plays a pivotal role in fostering the overall effectiveness of legal frameworks within Europe, consequently bolstering the foundations of the rule of law.


3. CRIMINAL LAW AND AI. THE MACHINE AS A TOOL OF JUSTICE

The influence of Artificial Intelligence permeates both of the domains of processual and substantial criminal law.

In the sphere of investigation and policing, Artificial Intelligence augments the efficacy of law enforcement through advancements in policing practices, including predictive policing, and the implementation of profiling methodologies such as facial recognition systems and biometric identification. Notably, these programs facilitate the identification of criminal risks and judicious allocation of resources to proactively forestall foreseeable criminal activities and curtail victimization: for example, the Keycrime program, developed based on the experiences of the Milan Police Headquarters, serves as an effective tool for predicting serial offenses, including robberies, fraud against the elderly, apartment burglaries, sexual violence, among others. Similarly, the XLAW program, devised by the Naples Police and deployed across various regions, is employed to forecast thefts and robberies. Furthermore, these AI applications are designed to enhance the accuracy of post-event perpetrator identification.

In the realm of the judiciary, Artificial Intelligence holds the potential to enable more comprehensive and nuanced evaluations of criminal defendants. These evaluations involve the cross-referencing of historical data concerning defendants and assessments of their subjective propensity for engaging in criminal behavior. In essence, these algorithms scrutinize factors such as socioeconomic status, family background, neighborhood crime rates, and employment status to render a purported forecast of an individual’s criminal risk, often presented on a scale ranging from “low” to “high”, or expressed as specific percentages. In essence, these algorithms serve as tools for analyzing extensive historical data, identifying recurring patterns, and generating assessments founded on a significantly more robust statistical basis than the human judgments that underpin traditional evaluations.


22 For a better in-depth analysis, see: Lorenzo Belenguer, *AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry*. in AI Ethics, Springer, 2, 4, 2022, pp. 771-787

Thus, the definition provided in the report by the EPIC, *Algorithms in the Criminal Justice System*, available at https://epic.org/algorithmic-transparency/crimjustice/, reflects this understanding.
3.1. The machine as a criminal tool

Criminal acts are pacifically defined as acts (or omissions) constituting offences punishable under criminal law, and recent studies have underscored the substantial impact of Artificial Intelligence across various domains of criminal activity.23

Notably, in the realm of finance, particularly within financial markets, there is evidence of the deployment of social bots—software that automates social media accounts and simulates human users—in schemes like “pump-and-dump” 24: these illicit schemes artificially inflate security prices by disseminating false, deceptive, or exaggerated information to create an artificial demand, ultimately enabling the sale of securities at elevated prices. Market simulations have also demonstrated that artificial trading agents, employing reinforcement learning—a machine learning technique predicated on rewarding correct choices—can acquire the practice of financial spoofing. This entails placing continuous orders over a defined period without any intention of executing them, with the primary objective of manipulating market prices.25

The importance of Artificial Intelligence crime as a distinct phenomenon has not yet been acknowledged. Until relatively recently, AI systems were constrained by predefined behaviors, operating exclusively through algorithms established by programmers. This included software engineered for purposes such as disabling a bank’s cybersecurity systems or causing destruction or damage to computer data. Assigning criminal culpability in such cases did not present significant challenges. Regardless of the complexity of the AI entity’s actions, responsibility ultimately rested with its controller or user. This is because AI entities lack cognitive agency and their behaviors adhere to predetermined patterns, thus being predictable. From this perspective, intelligent entities were perceived as mere instruments wielded by humans for the commission of crimes.26 Consequently, the concept of asset confiscation as a preventive measure could be applied to AI entities, even in the absence of a criminal conviction, as articulated in Article 240 of the Italian Criminal Code.27

24 T.C. King, Artificial Intelligence Crime, cit., 89 seq.
26 S. Riondato, cit., 85 seq.
27 Art. 240 Italian Criminal Code:
1. In case of conviction, the judge has the authority to order the confiscation of items that were used or intended for the commission of the crime, as well as the items that are the product or profit of the crime.
In light of these considerations, Italian law, in alignment with legal frameworks in other European Union member states, presently lacks definitions for crimes committed by artificial intelligence. The absence of dedicated regulations to address offenses perpetrated by autonomous AI agents underscores the pressing need for further legal development in this domain: this is crucial to ensure the establishment of appropriate mechanisms for accountability and regulation in response to the evolving landscape of technological advancements.

4. THE LEGAL FRAMEWORK OF CRIMINALITY

Today, the imposition of criminal penalties hinges upon two key prerequisites: first, the conduct must be previously proscribed (reserve of law), and second, that a judge administers the punishment. In the Italian legal system, these conditions are explicitly outlined in articles 13 and 25 of Italian Constitution.

To establish an act as a criminal offense, modern legal systems necessitate a minimum of two fundamental elements. The first element, known as *actus reus* (literally: the criminal act), mandates that the act aligns precisely with the criteria specified in the relevant laws. The second element, known as *mens rea* (literally: the criminal intent), comprises a range of mental states, with the highest level being voluntariness, sometimes coupled with intent or specific purpose. Lower mental

---

30 Art. 13, Italian Constitution:
1. Personal liberty is inviolable.
2. No form of detention, inspection or personal search is allowed, nor any other restriction of personal freedom, except by reasoned act of the Judicial Authority and only in the cases and by the manner provided for by law.
31 Art. 25, Italian Constitution:
1. No one can be diverted from the pre-established competent judge by law.
2. No one can be punished except in accordance with a law that was in force before the committed act.
3. No one can be subjected to security measures except in cases provided for by law.
32 Traditionally, Italian doctrine and jurisprudence deconstructs the crime into:
1. Objective element: This aspect of a crime pertains to the physical actions carried out by the individual, constituting the core material of the offense. It encompasses not only the physical aspects of the action itself, such as a physical assault or theft, but also any contextual factors that might be pertinent to defining the offense, such as the location, timing, or method employed.
2. Subjective element: The psychological state or intention of the individual committing the act. It encompasses *dolus*, which indicates a deliberate intention to engage in the conduct that constitutes the offense, as well as *culpa*, indicating a lack of diligence or care in the individual’s behavior that results in the commission of the offense.
3. Social (or merely legal) wrongfulness: This element represents the discrepancy between the act and the entire legal framework, extending beyond just the criminal domain. It reflects whether the action is in harmony with the broader legal system.
states include negligence (where a reasonable person should have known) and strict liability offenses\textsuperscript{33}. When it can be proven that an individual knowingly committed the criminal act or did so with criminal intent, that person is held criminally accountable for the offense\textsuperscript{34}.

The objective of this study is, \textit{prima facie}, to identify and summarize how to incorporate artificial intelligence into the domain of criminal law and, then, to analyze and deconstruct the atypical relation man-machine and its possible output as a criminal concurrence.

This paper will focus on the \textit{actus reus}, leaving the focus on \textit{mens rea} to another occasion.

\section*{4.1. The Actus Reus}

This section analyzes AI’s criminal liability using three models, as expounded by distinguished legal doctrine: the Perpetration-via-Another liability model, the Natural-Probable-Consequence liability model, and the Direct liability model.

\subsection*{4.1.1. The Perpetration-via-Another Liability Model}

The Perpetration-via-Another model pictures AI as an innocent agent, akin to a child: lacking autonomous will, the machine can be used only as a tool. The machine, in fact, just executes an order given by an human. In this scenario, only those who exploit the innocent agent are held criminally responsible as perpetrators-via-another.

Excellent doctrine\textsuperscript{35} argues that when AI entities are involved in a crime, they should be regarded as innocent agents devoid of human attributes. Consequently, AI entities are viewed strictly as machines and not active participants in the criminal act, whether as main actors or accomplices. In such cases, where the actual perpetrator lacks \textit{mens rea} (criminal intent), legal responsibility invariably falls upon the creator, programmer, or end-user of the Artificial Intelligence entity. Hallevy likens these circumstances to situations involving mentally limited individuals like children, mentally incompetent individuals, or those without a criminal state of mind. In these scenarios, the intermediary (AI entity) is considered a sophisticated tool, with the true perpetrator being the orchestrator of the crime, held accountable as the primary perpetrator\textsuperscript{36}.


\textsuperscript{34} As already highlighted in C. Piparo, \textit{Ibidem}.

\textsuperscript{35} G. Hallevy, \textit{The Criminal Liability of Artificial Intelligence Entities}, cit., pp. 179 e seq.

\textsuperscript{36} As already pictured in: Kemi Ogunnoiki, \textit{A Critique of Gabriel Hallevy ‘s Models of Criminal Liability of Artificial Intelligence Entities}, in International Journal of Comparative Law and Legal Philosophy 4 (3), 2022, pp. 4 seq.
But who assumes the role of the perpetrator-via-another? Two potential candidates are identified: the AI software programmer and the end-user. A programmer may intentionally design software for an AI entity with the aim of enabling it to commit specific offenses. For instance, a programmer might create software for an industrial robot and program it to set fire to a factory during unoccupied hours. Although the robot commits arson, legal liability is assigned to the programmer. Alternatively, an end-user can be seen as the perpetrator-via-another when they employ an AI entity without programming it themselves. For example, a user purchases a servant robot capable of executing commands from its master. The user instructs the robot to physically confront any intruders in their home. In this scenario, the robot carries out the assault, but the user is considered the perpetrator.

In both cases, the AI entity is the actual agent that committed the offense. However, since neither the programmer nor the end-user performed actions that align with the precise definition of the offense, they do not meet the actus reus requirement for that particular offense. The liability model of perpetrator-via-another treats the AI entity’s actions as if they were the actions of the programmer or end-user, grounded in the instrumental use of the AI entity as an innocent agent.

This liability model does not ascribe any mental capacity to the AI entity itself. Instead, it equates AI entities with inanimate objects or animals in terms of criminal liability. For example, just as a burglar using a screwdriver to break into a building does not render the screwdriver criminally liable. This model is particularly relevant in cases where AI entities are used instrumentally to commit offenses without utilizing their advanced capabilities or when outdated AI entities lack modern functionalities.

It is essential to note that “this model is not suitable when the software of the AI entity was not designed to commit the specific offence, but was committed by the AI entity nonetheless. The model is also not suitable when the specific AI entity functions not as an innocent agent, but as a semi-innocent agent.” The legal result of applying this model is that the programmer and the user are criminally liable for the specific offence committed, while the AI entity has no criminal liability whatsoever.

In legal terms, applying this model results in criminal liability for the programmer and end-user regarding the specific offense committed, while absolving the AI entity of any criminal responsibility.

37 See also: G. Hallevy, Ibid.; C. Piparo, Ibid.
38 G. Hallevy, Ibid.
39 K. Ogunnoiki, op. cit., p. 5.
40 K. Ogunnoiki, Ibid.
41 See also: For further analysis, N. Lacey, C. Wells, Reconstructing Criminal Law-Critical Perspectives on Crime and the Criminal Process, 1998; C. Piparo, Ibid.
42 C. Piparo, Ibid.
4.1.2. The Natural-Probable-Consequence Liability Model

The second model of AI entity criminal liability involves situations where programmers or users are deeply involved in the AI entity’s activities but don’t intend to commit offenses. Nevertheless, if the AI entity commits an offense during its normal operations, the natural-probable-consequence liability model may apply. This model holds individuals accountable for offenses that are a natural and probable outcome of their conduct, even if they had no actual knowledge of the offense.

For example, a user employs AI software designed to detect internet threats to safeguard a computer system it’s installed in. However, unbeknownst to the user, the AI destroys every external software recognized as a threat, inadvertently committing a computer offense.”

This form of liability is grounded in negligence and encompasses scenarios where programmers or users should have foreseen the possibility of an offense but didn’t intend for it to occur. It applies to individuals who were not the actual perpetrators of the offense but contributed to it intellectually. Reasonable programmers and users should have foreseen the offense and taken steps to prevent it, even though they didn’t intend for it to happen. However, the legal consequences vary depending on whether the programmers or users were negligent without criminal intent or knowingly and willfully used the AI entity to commit one offense, which resulted in another offense being committed. In the latter case, they can be held accountable for the offense as if it was committed knowingly and willfully.

However, as the above mentioned doctrine criticizes, the application of this model leads to two possible outputs. On the first side, if “the AI entity acted as an innocent agent, totally oblivious of the criminal prohibition, it is not held criminally accountable for the offence committed, as the action of the AI entity is not different from perpetration-via-another liability model. But if the AI entity did not act merely as an innocent agent, then, in addition to the criminal liability of the programmer or user, pursuant to the natural-probable-consequence liability model, the AI entity itself shall be held criminally liable for the specific offence directly.”

4.1.3. The Direct Liability Model

When applying the natural probable consequence liability model to AI entity criminal liability, two possible outcomes emerge. If the AI entity acted as an innocent agent, oblivious to the criminal nature of its actions, it won’t be held criminally liable for the offense it committed. This aligns with the first liability

---

43 G. Hallevy, op. cit., pp. 183-184
44 G. Hallevy, op. cit. pp. 184 seq.
model, where the AI entity is considered a tool used by others. However, if the AI entity didn’t act as an innocent agent and had knowledge of the criminal prohibition, it can be held directly and independently criminally liable for the specific offense it committed\(^{46}\). This direct liability model constitutes the third approach to AI entity liability and places the focus squarely on the AI itself. The determination of the AI entity’s liability hinges on whether it acted innocently or had knowledge of the prohibited conduct\(^ {47}\).

AI systems can receive sensory input and analyze factual data, similar to human understanding. They aim to mimic human cognitive processes, but specific intent, the strongest mental requirement, involves having a purpose or aim to achieve a particular outcome. For instance, in murder cases, specific intent refers to intending harm or death to a specific person. AI entities can be programmed with a purpose and take actions to fulfill it, demonstrating specific intent. Although humans have feelings that AI software cannot replicate, such as love or jealousy, these feelings are usually not necessary for most specific offenses. Many offenses only require knowledge of the external elements, and specific intent is only relevant to a few offenses. Therefore, the absence of such emotions in AI entities does not hinder imposing criminal liability\(^ {48}\).

If an AI entity fulfills all elements of an offense, it should not be exempt from criminal liability. Unlike certain segments of society like infants or the mentally ill, who have legal provisions exempting them from criminal liability, it is uncertain whether similar frameworks exist for AI entities\(^ {49}\). The criminal liability of an AI entity does not replace the liability of its programmers or users; rather, it is imposed in addition to their liability. The liability of an AI entity is not dependent on the liability of its programmer or user. If one AI entity is programmed or used by another, the liability of the programmed or used entity remains unaffected\(^ {50}\).

There is no reason to exempt AI entities or humans from criminal liability based on their collaboration. If an AI entity and a human act as joint perpetrators, accessories, or abettors, they should be subject to the corresponding criminal liability, regardless of their identity\(^ {51}\).

Negative fault elements and relevant defenses in criminal law is applied to AI entities, including self-defense, necessity, duress, or intoxication. Some adjustments may be needed when applying these defenses to AI entities, but fundamentally,


\(^{49}\) N. P. Padhy, cit., p. 10.

\(^{50}\) C. Piparo, *Ibid*.

the criminal liability of an AI entity, following the direct liability model, is similar to that of a human. It is based on the same elements and assessed in the same manner, with specific adjustments made in certain cases.52

4.1.4. Liability models in combination

The three liability models outlined above are not mutually exclusive, but rather, they can coexist and interact in various legal scenarios. For instance, when an AI entity acts as an innocent agent in the commission of a specific offense, and the sole director of that act is the programmer, the most suitable legal model for such a situation is the perpetration-via-another model (the first liability model). In this case, the programmer assumes liability for the AI entity’s actions as the perpetrator-via-another.

In the same scenario where the programmer is itself an entity (such as when one AI entity programs another AI entity to commit a specific offense), the direct liability model (the third liability model) would also apply alongside the first liability model. Thus, in such cases, the AI entity programmer could be held criminally liable, combining elements of the perpetration-via-another liability model and the direct liability model.

Similarly, if the AI entity takes on the role of the physical perpetrator of a specific offense, but the offense was not premeditated, the natural-probable-consequence liability model might be applicable. In this situation, the programmer could be considered negligent if the offense was not intentionally committed, or the programmer might be held responsible for the specific offense if another offense was deliberately planned, even if the actual offense committed was not part of the original criminal scheme.

However, it’s crucial to note that in cases where the programmer is not a human, the direct liability model must still be applied, in addition to the simultaneous application of the natural-probable-consequence liability model. Likewise, when the physical perpetrator is a human and the planner is an AI entity, a similar approach is necessary.

The interplay of these three liability models creates a unique legal landscape in the realm of AI entities and criminal law. Consequently, when AI entities and humans are involved, either directly or indirectly, in the commission of a specific offense, it becomes more challenging to avoid criminal liability. If the primary goal of imposing criminal liability is to maintain legal and social control within a specific society, then the coordinated application of all three models becomes essential in the context of AI entities.

Assuming that AI entities possess self-awareness, consciousness, and free will, their potential criminal responsibility comes into play. As AI entities can embody

social and ethical principles, being creations of humans, either directly or indirectly, this paper argues that there are adequate legal, juridical, and technological frameworks in place to recognize AI entities as active legal actors within the realm of criminal justice.

Finally, it is important to highlight that some, intelligent, doctrine thinks that to fill these gaps should be invoked company responsibility instead. Even though this is undoubtedly an original solution, this is not the place where such a theme should be discussed, due to its complexity.

5. PARTICIPATION IN MAN-MACHINE CRIMES

Traditionally, we refer to criminal participation when more than one person is involved in the commission of a crime. This occurs when there is not just one individual who fulfills the definitional elements of the criminal offense. Before starting to talk about the consequences of this interaction, it’s fundamental to draw the borders of such a phenomenon.

It’s evident that, if in the same context more than one person commits the same criminal action leading to the same criminal results, there will be participation. This is particularly evident in multi-individualistic crimes, that need more than one person to be committed (for example, art. 588 of Italian Criminal code punishes brawls). In such cases, the criminal conduct is (more or less clearly) tipifyed and punished. More questions arise in the case of atypical contributions: for example, why should be sentenced for a heist he who only threatens with a gun and he who just takes the wallet from a person? If we look at the causal contribution to the crime, nobody of those men committed a heist . Without entering such a theoretical dilemma we will rely on the main theory accepted by Italian doctrine and jurisprudence. Italian Criminal code introduces a new free-form and event criminal subtype by combining art. 110 c.p. and traditional criminal offenses.

So, in order to have criminal participation four elements are required: multiple agents, the commission of a typical criminal offense, a causal contribution of these multiple subjects and a peculiar that we will not analyze further in this context.

54 In order to dive deeper into the main theories see: Roberto Giovagnoli, Manuale di diritto penale – Parte generale, 2019, pp. 866 seq.
55 Art. 110 c.p.: When multiple individuals are involved in the same offense, each of them is subject to the penalty established for it, subject to the provisions of the following articles.
56 R. Giovagnoli, op. cit., p. 867.
57 R. Giovagnoli, op. cit., p. 868.
5.1. Participation with the machine

The institution of participation, so, becomes important due to the possibility to attribute to more people a typical crime instead of multiple atypical actions. And this is particularly true for the natural-probable-consequence and the direct liability models, since the first liability model simply represents a user-tool relationship between men and machines. This allows us to identify other subjects that intervene causally into the fact. In the case of The Natural-Probable-Consequence liability model, this would result into adding to a causal contribution the one of an AI machine. But, since here the responsibility is attributed to a third user and/or a programmer, this combination of liability model and criminal participation will result into abscribing the crime directly to the user/programmes as a participant.

Nonetheless, if we accept the configurability of a direct liability model, the same reasoning would result into considering the machine per se (and not through the user/programmer) as a participant. Also, if we accept the company responsibility theory, we should recognize as participant and responsible also the company.

5.2. Juridical limits of the concurrence

The institution of concurrence has multiple limits, if we try to apply something so different from traditional law thinking.

5.2.1. Mens rea

We can easily find one of these limits into the juridical institution of mens rea (or animus rei). Since we talked about a “peculiar” mens rea we find into the institution of criminal participation, it is important to distinguish into criminal participation where all participants have the same animus (for example: intentional participation into a brawl, which is intentional by definition) or different animi (for example: a non intentional pollution of toxic substances that are fraudently sold into the global market by another operator).

5.2.2. Same animus.

The vast majority of doctrine and jurisprudence peacefully accepts criminal participation where animi are the same. On one hand, the subjective element of joint participation consists of two components: the “awareness of cooperating with others in the commission of the typical act [...] must be added to the representation and intention of the act, which are required, according to general principles, for the configuration of an intentional offense”\(^{58}\). On the other hand, art. 113 of Italian

\(^{58}\) Mario Romano, Giovanni Grasso, Commentario sistematico del codice penale, 3\(^{rd}\) ed., II, 2005, p. 180.
criminal code governs cooperation in cases of culpable crimes, which occurs when multiple individuals engage, mutually aware of their contribution to another person’s action or omission, in a specific autonomous conduct leading to the occurrence of an unintended event, not desired by any of the co-operators.\textsuperscript{59} This provision pertains to activities involving various subjects that are somehow interconnected and does not demand that each, individually, be theoretically capable of committing the offense. However, each must provide a legally appreciable causal contribution to the realization of the unintended event by the individuals obliged to comply with precautionary regulations.\textsuperscript{60} This is a case where the joint participation man-machine is theoretically acceptable.

5.2.3. Different animus.

There is a question of whether the additional requirement of a common intent among participants is necessary, which presupposes that all participants have mutual awareness and intent to cooperate with each other in the commission of the act. According to modern doctrine, this shared intent is not necessary for all participants. In fact, unilateral participation is allowed – intentional participation in a culpable crime – carried out by someone who, through an atypical intentional act, exploits the negligence of other participants, using them as if they were mediated perpetrators. Arguing for the possibility of intentional participation in a culpable crime has significant practical implications, as it allows for the prosecution of atypical behaviors that would otherwise go unpunished.\textsuperscript{61} This is the second case where the joint participation man-machine is also acceptable.

5.2.4. Culpable participation into voluntar crime

This case is way more problematic. The major orientation doesn’t accept the culpable participation into voluntar crimes. This should limit the culpable participation of the user, the programmer or the company, since this participation is not accepted. At most, the culpable participant could be punished for a different crime if it is punished by law as it is.

The historical debate can be essentially visualized as a triangle with three vertices. Here are the three aspects.

According to the first aspect, art. 42, par. 2, of code Rocco states that “No one can be punished for an act provided by law as a crime unless they have committed it intentionally, except in cases of pre-intentional or negligent crimes expressly

\textsuperscript{59} Cass., SSUU, sent. n. 5 of 1999.
\textsuperscript{60} Cass. pen, Sez. fer., sent. n. 41158 del 2015.
\textsuperscript{61} See. R. Giovagnoli, op. cit., pp. 888 e seq.
provided for by law”. It requires the express provision for negligent liability, which seems to be lacking for complicity in intentional crimes. It’s argued that this provision only refers to the special part of the code, therefore only to the incriminating specifications of individual acts. The literal wording supports this direction, as the act that is expressly provided for as a crime by law must be the subject of negligent liability.\footnote{Paolo Piras, Svanisce il concorso colposo nel reato doloso, in Dir. pen. cont., 3, 2019, p. 7.}

According to the second aspect, it is believed that complicity in intentional crimes cannot be configured since art. 113 limits negligent participation to the sole hypothesis of negligent crimes. The clear literal expression with which the text begins ("In negligent crimes") would not allow for the inclusion of intentional crimes. It is countered that this is not decisive for excluding configurability, given that the provision revolves around an event caused by the cooperation of multiple people, which constitutes the core without specifying a psychological element.\footnote{Cass. Sez. IV, sent. n. 39680 del 2002.} It is also believed that art. 113’s expression “In negligent crimes” would also encompass intentional crimes because of Marinucci’s doctrinal statement that “there is no intent without negligence”. This allows for the argument that intent is not something different from negligence but something more, involving not only the violation of an objective duty of diligence but also the consciousness and will of the event. However, this objection has been criticized by doctrine and jurisprudence, which correctly observe that Marinucci’s expression “non c’è dolo senza colpa” wasn’t suitable at all for this occasion, since Marinucci was speaking about the essence of 

culpa and dolus per se and not speaking about technical configurations of criminal participations. Indeed, the Author only wanted to emphasize that there is a common basis for intent and negligence, constituted by the violation of an objective duty of diligence, while intentional and negligent acts give rise to structurally different types of offenses.\footnote{Giorgio Marinucci, Non c’è dolo senza colpa. Morte dell’ “imputazione oggettiva dell’evento” e trasfigurazione nella colpevolezza?, in Riv. it. dir. proc. pen., 1991, pp. 3-39.}

According to the third aspect, law systems punish several cases of negligent facilitation of intentional crimes (for example, art. 254 of code Rocco). This would be superfluous if complicity in intentional crimes could be configured in general terms. However, the counterargument is straightforward: the separate provision may be dictated by other reasons, not just incrimination (for example, the legislative intention to provide a particular penalty.\footnote{P. Piras, op. cit., p. 8.})

It’s clear that agreeing to the major orientation would result into strongly limiting company, programmer, and user responsibility.
6. CONCLUSIONS

To conclude, it’s evident that machine’s liability is something *per se* ambiguous.

Nonetheless, we can assess that machine can be – at least indirectly – criminally liable by human’s mediation, that uses or acts with the machine itself.

While speaking about autonomous machine’s responsibility is extremely complex and deserves an autonomous occasion and a decent in-depth analysis, it’s evident that AI can commit crime and that same crime can be referrable to different people.

So, when we talk about machine liability we mostly talk about two dimension: the first, historical naturalistic, that focuses on the natural deed from the AI that commits a crime, and the second – juridical and philosophical – that focuses on criminal liability. In this second case, it appears problematic to ascribe criminal responsibility to a machine itself, leading this to a different question: *machina puniri potest?*

REFERENCES

Bibliography:


Fabio Basile, *Intelligenza artificiale edirito penale: quattro possibili percorsi di indagine*, in Diritto Penale e Uomo, 2019


Lorenzo Belenguer, *AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry*. in AI Ethics, Springer, 2, 4, 2022;


Antje du Bois-Pedain, *Participation in Crime*, in University of Cambridge Faculty of Law Research Paper, 6, 2019;


Joshua Dressler, *Cases and materials on Criminal law*, 1999;

Roberto Giovagnoli, Manuale di diritto penale – Parte generale, 2019;
Carlos Ignacio Gutierrez, Anthony Aguirre, Risto Uuk, Claire Boine, Matija Franklin, A Proposal for a Definition of General Purpose Artificial Intelligence Systems, 2022;
Giuseppe Francesco Italiano, Intelligenza artificiale: passato, presente, futuro, in Francesco Pizzetti (editor), Intelligenza artificiale, protezione dei dati personali e regolazione, 2018;
William Samuel Isaac, Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice, in Ohio St. J. Crim. L., 2018;
Thomas King, Nikita Aggrwal, Mmariasrosia Taddeo, Lorenzo Floridi, Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, in Science and engineering ethics, 2019;
Joost Kok, Egbert Boers, Walter Kosters, Peter van der Putten, Mannes Poel, Artificial Intelligence: Definition, Trends, Techniques and Cases, in Knowledge for sustainable development: an insight into the Encyclopedia of life support systems, 2002;
Vittorio Manes, L’oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia, in Discrimen, 2020;
Giorgio Marinucci, Non c’è dolo senza colpa. Morte dell’ “imputazione oggettiva dell’evento” e trasfigurazione nella colpevolezza?, in Riv. it. dir. proc. pen., 1991;
Narayana Prasad Padhy, Artificial intelligence and intelligent systems, in Oxford University Press, 2005;
Carlo Piparo, Machina delinquere potest? A modern criminalization challenge due to lack of text, in Text, context, and subtext in law, 2023;
Paolo. Piras, Svanisce il concorso colposo nel reato doloso, in Dir. pen. cont., 3, 2019;
Mario Romano, Giovanni Grasso, Commentario sistematico del codice penale, 3rd ed., II, 2005;
Roger Carl Schank, What’s IA, Anyway?, in IA Magazine, 8(4), 1987;
Haroon Sheikh, Corien Prins, Erik Schrijvers: Definition and Background, in Mission AI. Research for Policy. Springer, 2023;
Silvio Riondato, Robot: talune implicazioni di diritto penale, in Paolo Moro, Claudio Sarra (edited by), Tecnodiritto. Temi e problemi di informatica e robotica giuridica, Milano, 2017;
Federico Stella, Giustizia e modernità. La protezione dell’innocente e la tutela delle vittime, 2003.
Карло Пипаро
Универзитет у Удинаму
carlopiparo@gmail.com
ORCID ID: 0009-0009-7965-0770

Модели кривичне одговорности кривичног учешћа у дигиталном окружењу – перспективе савремених изазова у италијском конституционализму

Саждењак: Убрзан напредак и распростирање информационо-комуникационе технологије (ИТТ) увели су нас у свеобухватну друштвено-правну трансформацију. Од многих револуционарних напредака, вештачка и интелигенција је се кључна сила, прожимајући свакодневни живот. Од царства трговине и индустриских злочина до здравствене заштите, технологија вештачке интелигенције је била неопходно средство обликовања начина на који комуникација, радимо и крећемо се у свемиро око нас. Са њеним чудесним могућностима и све јачим домаћима, вештачка интелигенција освајаје као завештање човечанској немилосрдној тежњи за иновацијама и безграничном могућностима, које могу да извршавају злочине у свечаном окружењу. Док обављају своју улогу, могу да предузимају радње, које могу да резултују у злочине којима је неопходно одговорност заснована на њеним могућностима и домени."
Ииак, јпир ђоро ђоменўша мовела одговорносин оиўарах врала ёйоиуно савременом сценарии: конкуренциносин човека и машине (иодуарносин између човека и алгоришима вештачке интелигенције). У сиива, ако дефинисање одговорносин машине долази са изазовима, још је комеликованије ирилдријин савременим усивавима иодуарносин између живој и дигиталног. У сиива, јпиребно је іроценизи да ли машина може да чини злочине (или је шо само инструменци), уијердрији како се машина може слайди са човеком и колика је одговорносин на њу. Овим радом се желе анализирајти карактрисеинке вештачке интелигенције, разрадићи јпир могућа мовела одговорносин вештачке интелигенције и, на крају, дефинсази злочиначко учешће човек-машина кроз соција италјанскога ђрава.

Кључне речи: одговорносин, злочиначка намера, ђарицициација, ђрође-мер, алгоришим, кривично ђраво.

Датум прихватања рада: 3.1.2024.