THE INTERSECTION OF AI, IOT, AND CRIMINAL LAW: A TECHNOLOGICAL AND LEGAL REVIEW

Claudio D. Amorelli[*], Gabriele Lecce[**]

SOMMARIO: 1.- Introduction; 2.- AI and Criminal Law: Some Applicative Lines; 3.- Outline of the Prevention of Negligent Offenses in the Intersection Between AI and IoT; 4.- AI-IoT devices for crime detection and risk prevention; 5.- Security challenges in IoT-based Smart Cities; 6.- Predictive Justice: Critical Observations and Regulation Between Prevention and Commensuration.

1.- **Introduction.**

Wanting to draw a directive line between the study of regulatory systems and a technical-engineering type of analysis, one solution would come from the tools we possess in the sphere of punitive principles[1].

Moving within the confines of the criminal subject matter makes it possible to make use of the instrumentarium coming from the dynamics of general prevention in negligent offences matters, a negligent standard that has led part of Italian doctrine to propose[2] a reference to new technologies in the general-preventive logic that criminal systems need in order to survive, especially in the social complexity of contemporary democracies[3].

In short, the cue concerns the obligations to conform to the precautionary standard to prevent the illicit risk in the negligent nature of the conduct, a risk that can be cancelled in the presence of automated decisions or reduced in the presence of a summation between personal action and digital action; here the two sides of the coin on the one hand, the advancement of new technologies brings with it the reduction of social risks, the presence of "conveniences" also legal (greater security of evidence[4], celerity of application in contractual matters), while on the other hand, the prospect of integration between AI and IoT reduces the range of aleatoriness that characterises law in its factual existence[5].

If it is therefore necessary for the jurist, especially in criminal law, to come to terms with the dynamics of AI[6] in the construction of a new preventive perspective, it is essential to shift from the classic

[*] Master's degree in Law at Università di Firenze – Dipartimento di Scienze Giuridiche, Florence, Italy, "Esperto esterno ex art. 45" in Philosophy of Law at Università degli Studi di Milano – Dipartimento di Scienze Giuridiche "Cesare Beccaria", Milano, Italy.

[**] Master's degree student in Telecommunication Engineering at Politecnico di Milano – Dipartimento di Elettronica, Informazione e Bioingegneria, Milano, Italy.

[1] And this is not due to a preference for studies in positive law, but rather with the aim of identifying the fundamental principles underlying individual liability. See on punishment F. Palazzo, R. Bartoli, *Corso di diritto penale. Parte Generale*, Torino 2023, 13ss.; F. Mantovani, G. Flora, *Diritto penale. Parte Generale*, Padova 2023, 677ss.

[2] L. Cornacchia, *Responsabilità colposa: irrazionalità e prospettive di riforma*, in *Arch. pen.* 2 (2022) 672ss.

[3] S. Aleo, *Diritto penale e complessità. La problematica dell'organizzazione e il contributo dell'analisi funzionalistica*, Torino 2009, *passim.*

[4] On the general issue of scientific evidence and the validity of its scientific nature in its formation, see *ex multis* G. Carlizzi, G. Tuzet (ed.), *La prova scientifica nel processo penale*, Torino 2018. On digital evidence, see S. Pietropaoli, *Informatica criminale*, Torino 2022, 85ss.

[5] F. Cordero, *Gli osservanti. Fenomenologia delle norme*, Milano 2024, 348ss., on the 'lived' [vissuto] of normative experience.

[6] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo* september 29th (2019) 2ss.

commensurative approach to a strictly reductive approach regarding the scope of human action (control over the fact)[7].

To achieve this, it is necessary to: 1) adopt a secular approach to new technologies, considering the applicable spaces through the lens of those involved in their construction, training, and distribution; 2) consider the criminal offenses, here incriminatory, from the perspective of conduct orientation, including organizational conduct (an insight might come from recent interpretations of Article 113 of the Italian Penal Code)[8]; 3) keep in mind the rethinking in terms of commensuration-proportionality and the reduction of the validity scope of what "law" is[9].

Although currently the intersection between AI and incriminatory offenses has only touched upon the financial sector[10], thus making any reasoning in positive law that disregards this important micro-system of artificial criminal law clearly in contrast with the typicality of type of offence in criminal law, the reversal of the approach towards a preventive line would be allowed by tools provided by the presence of organizational functions already in the recent AI regulatory legislation.

An immediate reference comes from the so-called AI Act (Regulation No. 1986/2024), through which the European Commission sets out, albeit according to a strictly anthropocentric approach[11] (which fits well with the premises of this inquiry), a foundation for the interpreter to analyze the current applicative challenges. Indeed, the regulation of the risk inherent in the application of artificial intelligence systems (Article 25) allows for looking at the risk threshold beyond which criminal intervention will be necessary (and desirable)[12].

Italian legislation in this area, following the ideal political line fully aware of the risks associated with the lack of flexibility in such a dynamic field as new technologies, is moving with a delegation law framework (No. 1146/2024) that aims to adapt the foundations of the AI Act to our legal system.

It seems, in any case, that both from the perspective of machine usage and from the perspective of "subjectivization" towards them, the key word is risk. Therefore, in addition to those related to criminal profiling and penalty enforcement, suggestions from the theory of fault could help reconstruct applicative directions useful for reconciling the most recent intersection between person and law, and person and machine.

An example of integration between IoT systems and AI is the smart city, an urban area that enhances its services by seamlessly integrating in its infrastructure Information and Communication Technologies (ICT). The need for this new paradigm of city derives from the growing trend of urbanization and energy consumption of the global population, as well as new standards of quality of

---

[7] M. Di Florio, *Il diritto penale che verrà. Brevi considerazioni sul possibile impiego dell'IA per prevenire il rischio di disastri colposi*, in *Arch. pen.* 2 (2021) *passim.*

[8] F. Consulich, Errare commune est. *Il concorrente colposo, il nuovo protagonista nel diritto penale di impresa (e non solo)*, in *Leg. pen.* march 23th (2022) 2ss., 21ss.

[9] The 'ability to choose' see Cordero, *Gli osservanti* cit. 352ss.

[10] F. Consulich, *Il diritto penale al tempo dell'intelligenza artificiale. Prospettive punitive nazionali dopo l'AI act*, in *Diritto di difesa* december 17th (2024) 1s. See also the contributions on the procedural sector of investigations by F. Di Vizio, *Prevenzione e investigazioni: l'uso di IA, big data e soluzioni tecnologiche in ambito finanziario e nel contrasto del riciclaggio (AML) e al finanziamento del terrorismo (CFT)*, in *disCrimen* january 11th (2024) *passim*., as well as the considerations in F. Consulich, *Intelligenza artificiale e reati finanziari*, in F. Consulich (ed.), *Reati in materia bancaria e finanziaria*, Torino 2024, and – with particular focus on cryptocurrency matters – in Basile, *Crypto assets e responsabilità penale*, in F. Consulich (ed.), *Reati in materia bancaria e finanziaria*,

[11] M.G. Peluso, *Introduzione*, in M.G. Peluso (ed.) *La regolazione europea dell'intelligenza artificiale. Primi commenti per una guida alla comprensione dell'AI Act*, in *Ciberspazio e Diritto. Rivista Internazionale di Informatica Giuridica* 3 (2024) 403.

[12] Consulich, *Il diritto penale* cit. 12-14. Cf. C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.* 4 (2019) 1909ss.

life that are inseparable from modern technologies. To face these challenges, cities require an efficient and autonomous way of managing their resources. The help can come from the building blocks of smart cities, Internet of Things (IoT) devices, which can be easily deployed in the cities infrastructures to collect data and to interact with the surrounding environment through their sensors and actuators.
In order to analyze the large flows of data generated by the devices of the smart cities, the use of Artificial Intelligence (AI) algorithms and of appropriate communication technologies is of fundamental importance. These kinds of algorithms can make predictions on the future status of the city infrastructures and services, and can facilitate, or make autonomous, the traditional decision-making process of a worker. Typical applications of AI-enhanced devices can be smart water supply, waste and energy management, mitigation of environmental pollution, traffic management, and predictive maintenance of city infrastructures such as bridges, buildings and roads[13].
The role of AI is not just limited to the analysis of data received from the networks end-devices, but can be also integrated into communication protocols to manage and optimize wireless networks. As a matter of fact, the emerging 5G networks will not be enough to flawlessly withstand the low latency and high reliability requirements of ultra-dense areas like smart cities[14], because the interconnected environment of IoT devices and its derivatives such as Internet of Drones (IoD), Internet of Vehicles (IoV) and Internet of Medical Things (IoTM) need continuous connectivity to work properly. To achieve maximum quality of service (QoS), 6G networks are being designed to integrate AI for real-time optimization of wireless networks, assuring services such as autonomous driving, smart city surveillance and remote surgery[15]. Although the use of 5G and 6G, or in general, classical cellular networks, ensure the connectivity requirements of smart cities, they are not suitable communication technologies in terms of power consumption for simple IoT devices. IoT networks typically use communication technologies specifically designed for IoT systems, like ZigBee and Bluetooth Low Energy for short range connectivity or LoRaWAN and NB-IoT for long range.
AI-IoT systems can also be used as a crime detection tool to identify criminal activities or to predict incidents. While these applications have great potential in improving the quality of life and the safety of a smart city, they also raise concerns about privacy and data security of the users[16]. In fact, smart cities are complex and heterogeneous technological environments in which various types of cyber-attacks can be performed to undermine the data transmitted from their devices. Moreover, while most of these attacks can be overcome with conventional security solutions, IoT devices are usually resource-constrained, and cannot easily trade off performance for security[17]. To enable, for example, encryption of data, we must assure that the device can handle higher data rates without restrictions on its expected lifetime. It's important to emphasize that AI techniques can also be exploited from the side of device manufacturers and service providers to gather sensitive information about their users. For example, using data mining techniques based on machine learning, it is possible to predict the location or the mobility patterns of a user from the data collected with smart mobility applications.

[13] M.E.E. Alahi et al., *Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends*, in *Sensors* 23.11 (2023) 5206.
[14] S. Islam et al., *Mobile Networks Toward 5G/6G: Network Architecture, Opportunities and Challenges in Smart City*, in *IEEE Open J. Commun. Soc.* (2024) 1.
[15] L. Ismail, R. Buyya, *Artificial Intelligence Applications and Self-Learning 6G Networks for Smart Cities Digital Ecosystems: Taxonomy, Challenges, and Future Directions*, in *Sensors* 22.5 (2022) 5750.
[16] Z. Ullah et al., *Applications of Artificial Intelligence and Machine learning in smart cities*, in *Computer Communications* 154 (2020) 313ss.
[17] H. Habibzadeh et al., *Sensing, communication and security planes: A new challenge for a smart city system design*, in *Computer Networks* 144 (2018) 163ss.

2.- **AI and Criminal Law: Some Applicative Lines.**

Article 3 of the aforementioned AI Act provides the interpreter with a definition of artificial intelligence. Overcoming this "gray zone" of conceptual ambiguity helps eliminate one of the interpretative problems at the intersection of law and AI, namely the absence of definitions of both concepts, and thus the vagueness of the applicable spheres of law whenever new algorithmic technologies are used, "to have machines perform complex tasks previously carried out by humans."[18]

Article 3 states:

'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

Thus, by excluding with this definition any reasoning concerning the autonomy of such systems[19], a functional approach allows for delineating the applicable spaces in the incriminatory offenses concerning the precautions for those who use them.

Starting from the current regulation, the testing ground, as mentioned, comes from the field of financial crimes, where, due to the development of digitized financial services, the legislator's attention has focused on defining how artificial intelligences can commit crimes, as they—if left unchecked—are more inclined to seize advantageous opportunities beyond the value system underlying the incriminatory offense[20]. The speed, or rather immediacy, of these systems allows for an undeniable economic advantage but reduces the space for control. Indeed, this is the conflict at the heart of the regulation of the risks associated with the use of AI, especially when, as in our case, such tools are not seen as potential perpetrators of the crime but as instruments for its prevention and, consequently, the repression of behaviors perceived as criminal by the machine.

In the ideal dimension of the integration between AI and IoT, three macro-sectors take on particular relevance: cybersecurity in a broad sense[21], traffic accident crimes, and the discipline of labor criminal law, in which, for completeness, the recent regulation in the medical field is also included (due to similar applications).

The regulation related to traffic accidents intertwines with that of smart cars. Although there is still a lack of concrete scenarios for fully autonomous driving cars[22], advances—especially in software—within the complex architecture of autonomous vehicles point to a particular external communication organization for these vehicles with the AI tools surrounding them, making them a typical development target for cyberattacks and for verifying illicit acts (not only negligent ones[23]) of various

[18] European Commission for the Efficiency Of Justice (CEPEJ) European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, Appendix III, Glossary (2018), 69. Cf. on the notions of "strong" e "weak" AI, G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.* 4 (2020) 76ss. Cf. C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.* 4 (2019) 1911ss.; M. Á. Cuadrado Ruiz, *Diritto penale e salute di fronte alle tecnologie emergenti e all'intelligenza artificiale: una prima approssimazione*, in *Studi senesi* 2 (2023) 259-262.

[19] Consulich, *Il diritto penale* cit. 10.

[20] Id., *Intelligenza artificiale* cit. 238ss.

[21] See *infra* §5.

[22] For general considerations, see G. Calabresi, E. Al Mureden, *Driverless cars. Intelligenza artificiale e futuro della mobilità*, Bologna 2021, *passim.*

[23] Such specification is due to the attention, deserved in recent years, given to the specification of the generality of negligent offenses, which led to the creation of the well-known offense of vehicular manslaughter (negligent homicide) [Article 589 bis Italian Penal Code], paving the way for similar proposals to specify negligent offenses also in labor law.

kinds affecting all road traffic participants[24]. At the European law level, the Cybersecurity Act of 2019 provides a guideline for a secular and non-catastrophic approach to the risks posed by smart tools in the classic sectors just listed. Indeed, according to Article 2.1 of the Act (Reg. 2019/881), the notion of cybersecurity "means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"[25].

Due to this approach, it is essential to focus on the methodology of attacks to which smart vehicles may be subject, considering their progressive increase in use in a society that is widely connected to the IoT. Indeed, the identified vulnerabilities primarily concern the appropriation of vehicle operational data and the potential alteration of its use[26]. As highlighted by experiments conducted by so-called ethical hackers[27], even the mere purpose of stealing operational data can seriously jeopardize the safety of all road traffic participants. Currently, criminal protection against unauthorized access (Article 615-ter of the Italian Penal Code) allows for adaptation to the needs of the complex IT system that characterizes smart vehicles. In fact, the provision in paragraph 2, number 3, which includes as an aggravated criminal offense "the destruction, damage, or theft, including by reproduction or transmission, or the inaccessibility to the owner of the system, or the interruption, in whole or in part, of the operation of the computer system, or the destruction or damage of the data and programs contained therein"[28], allows for expanding protection to cases of negligence resulting from intrusion into the onboard system that causes malfunction, leading to criminal traffic offenses.

Parallelly, according to recent doctrinal reflections, any attack capable of endangering road traffic would, following Article 432 of the Italian Penal Code and hoping for the introduction of specific autonomous or circumstantial incriminatory offenses, merit criminal repression if it alters or jeopardizes the fundamental functions of driving and the ability to interact with the road environment[29]. Finally, in closing this first approach to the subject, there is the potential for hijacking smart vehicles, a hypothesis that could, at least currently, be seen as unrealistic if it involved mass hijacking, but nevertheless is rare in its occurrence since, to date, the presence of a driver on board is still necessary. In any case, such hypotheses, it is noted, would already be subject to criminal protection under the offense of disaster (Article 434 of the Italian Penal Code) if there is an actual threat to the legal assets of life or personal integrity[30]. It should be emphasized that, fundamentally, the possibility of hijacking a vehicle allows the event to be qualified under the offense of kidnapping (Article 605 of the Italian Penal Code) or, as always, recourse to closing offenses, such as private violence (Article 610 of the Italian Penal Code), without the need for specific interventions *de lege ferenda*. Concerning the prevention of cybercrimes in the automotive sector, Italian legislation finds

[24] I. Salvadori, *Minacce alla* automotive cybersecurity *e tutela penale della sicurezza dei trasporti*, in *Arch. pen.*, 1 (2025), 2-4.

[25] Cf. Salvadori, *Minacce alla automotive cybersecurity* cit. 8, note 24. With reference to Italian legislation, D. Lgs. 138 of september 2024, implementing Directive (EU) 2522/2022, the so-called NIS 2, see Pietropaoli, *Informatica criminale* cit. 102ss.

[26] Salvadori, *Minacce alla* automotive cybersecurity cit. 22.

[27] Global Automotive Cybersecurity Report, 2024.

[28] Salvadori, *Minacce alla* automotive cybersecurity cit. 25.

[29] M. Lanzi, *Self-driving cars e responsabilità penale. La gestione del "rischio stradale" nell'era dell'intelligenza artificiale*, Torino 2023, 109ss; Salvadori, *Minacce alla automotive cybersecurity* cit. 30-32. The author rightly notes that, in reality, the provision of Article 432 alone allows for the repression of such behaviors and that, therefore, a more specific offense would serve no other purpose than symbolic criminal law. It would, instead, be more useful – contrasting with the anachronistic relevance of only public transport in the object of protection – to adapt the offense to the purposes of private vehicle usage.

[30] *Ex multis* A. Pagliaro, *Principi di diritto penale. Parte generale*, Milano 2020, 270ss.; Salvadori, *Minacce alla automotive cybersecurity* cit. 33ss.

adequate criminal hypotheses in the hope of an integrated criminal science aligned with the goals of cybersecurity[31].

Shifting attention to the field of (criminal) labor law, the disciplinary references in the AI Act become relevant. Even here, momentarily leaving aside prevention concerns, it is necessary to provide some functional information for the internal regulation of work organization. Indeed, the definition in Article 3, paragraph 1, number 1), together with Recital 48, enables the updating of the meaning of an AI system in relation to fundamental rights, including workers' rights[32]. While the immediate consequence of this is the management control of algorithms tasked with hiring or firing decisions for anti-discriminatory purposes, human oversight of the outputs, and system log retention obligations... what is significant is that human intervention imposes control not only on employers (represented here by the category of deployers) but also on the individuals subject to algorithmic decisions (cf. Article 26, point 7)[33]. AI must indeed promote transparency and improve working conditions, rather than serve as a tool for regression in the face of these rights. This is the guiding principle of Italian national legislation, which (draft bill 1146/2024) insists on the need to "improve working conditions, safeguarding the psycho-physical integrity of workers, in balance with work performance productivity." (Article 10). This assumption, affecting not only the issue of non-discrimination and the protection of personal data of individuals subject to algorithmic decision-making and control, is relevant in two areas: 1) the tendency towards parity of training obligations and thus control in the work dynamics (among all individuals regardless of hierarchy), and 2) risk assessment from activities based on the communication of information by worker representatives.

In fact, the trend of the judiciary to increasingly identify new guarantors in situations of intersection between fault and criminal omission has not yet directly impacted labor law, but—hypothetically—the abstract informational parity regarding the submission of one's data to an algorithmic process would allow for a process of accountability in relation to the control of risky activities thanks to control systems (especially audiovisual), then analyzed by machines to assess work-related or even criminal negligence, regardless of the supervisory work hierarchy[34].

Lastly, the intersection with the micro-system of medicine and criminal law: the field of medical liability is, in fact, a clear testing ground in discussions on criminal prevention and the updating of informational obligations and will be even more so when algorithmic use becomes predominant. Thus, the need for regulation arises, as in the most recent proposal (Articles 7, 8, 9, 22 of draft bill 1146/2024), which, in addition to integrating provisions suitable for non-discrimination in access to healthcare services and improving the living conditions of people with disabilities (Article 7, paragraphs 1-4), aims to regulate human intervention in the face of algorithmic assistance in healthcare activities as a whole: both in prevention, diagnosis, and care, where it is emphasized that the final decision is always entrusted to healthcare professionals (Article 7, paragraph 5), and (in the

[31] This is the conclusion of the most recent work on the topic: Salvadori, *Minacce alla automotive cybersecurity* cit. 35.

[32] M. Pizzocri, *Il tentativo di regolazione sistematica dell'Intelligenza artificiale nel diritto del lavoro, la normativa comunitaria Reg. 1689/2024 (AI Act) comparata col disegno di legge nazionale, e primi approdi giurisprudenziali*, in M. G. Peluso (ed.), *La regolazione europea dell'intelligenza artificiale. Primi commenti per una guida alla comprensione dell'AI Act*, in *Ciberspazio e Diritto. Rivista Internazionale di Informatica Giuridica* 3 (2024) 458ss.

[33] Id., *Il tentativo di regolazione sistematica dell'Intelligenza artificiale* cit. 460-462.

[34] See F. Consulich, *Manuale di diritto penale del lavoro*, Torino 2024, 40ss., 70ss., especially 107 on doubtful cases such as the case of the person responsible for the prevention and protection service (see Cass. sez. IV, 25/09/2023, n. 38914) and R. Blaiotta, *Diritto penale e sicurezza del lavoro*, II ed., Torino 2023, 29-78. This reference to the manuals is functional to the analysis of the trend toward rationalizing personal criminal liability in the dynamics of labor criminal law. In fact, while positions of guarantee still leave room for paternalistic application, they are increasingly adapting to the dynamics of informational obligations, according to a negligent standard based on concrete dominability.

following paragraph) that risk reduction activities must always be subject to subsequent human control[35]. The proposed intervention also touches on the issue of personal data processing (Article 8) and cybersecurity related to health record data (Article 9). Of potential interest to the analysis of this issue is the need for "digital literacy" and awareness of the risk inferred from Article 22[36].

Now, in light of this regulatory proposal, the issue—using the intersection between information and risk—shifts to negligence as concretely verifiable by the operator using such systems and how the machine might be capable of preventing a medical risk, both in the preventive stage and during healthcare delivery[37], especially where the operator uses specific tools for tracking the patient's health[38].

Indeed, full reliance on such diagnoses raises obvious risks regarding the qualification of criminal liability: even today, with positive law alone, techniques for exemption from liability (*ex multis* Article 590-sexies of the Italian Penal Code) raise important issues regarding the limits of medical liability autonomy. These issues, when intersected with the introduction of predictive systems—no matter how fine-tuned by experience—will not allow for a more precise evaluation of the medical decision-making autonomy space, risking expanding the scope of slight negligence. Indeed, an initial preventive space for accountability arises from the idea of resorting to administrative sanctions law to assess the improper use of AI systems and impose financial penalties in cases of violation and exceeding the "risk—predicted and foreseeable" (cf. the definitions currently available in the AI Act[39])[40].

Although the anthropocentric tendency, which drives recent European and national legislation, looks with hopeful eyes at human activity, one should not underestimate scenarios, here only briefly mentioned, in which AI systems could, in and of themselves, operate independently of human activity and interact with each other in a criminogenic manner, either intentionally or negligently, committing crimes as already occurs in the regulation of financial criminal law[41].

3.- **Outline of the Prevention of Negligent Offenses in the Intersection Between AI and IoT.**

The issue of tracking is closely intertwined with the question of criminal profiling in the prevention of crimes (especially negligent ones). Indeed, the anthropocentric view in recent AI regulation can be instrumentally reconsidered with the aim of enhancing the allocation of risk according to organizational parameters.

---

[35] B. Romano, *Il DDL in materia di IA: l'utilizzo nell'attività giudiziaria e in ambito sanitario*, in *Riv. it. med. leg.* 1 (2024) 413.

[36] Id., *Il DDL in materia di IA* cit. 414-416.

[37] Cuadrado Ruiz, *Diritto penale* cit. 262ss.

[38] Relatively to the intersection with IoT or with the tracking activity of so-called "biosensors" capable of obtaining real-time information about specific health conditions, see Ead., *Diritto penale* cit. 267.

[39] A. Rossetti, *Classificazioni e categorie di rischio nell'AI Act*, in bnews.unimib.it/blog/classificazione-e-categorie-di-rischio-nellai-act/, viewed 16 march 2025.

[40] Cuadrado Ruiz, *Diritto penale* cit. 272-275. The reference, drawn from the powers of the Personal Data Protection Authority, pertains to specific Agencies for the Supervision of Artificial Intelligence, already implemented in Spain with Royal Decree 729/2023. In Italy, the potential role could be assigned to the National Cybersecurity Agency. see https://www.lextech-hub.com/post/supervisione-e-sicurezza-dell-intelligenza-artificiale-il-possibile-ruolo-dell-acn-nell-attuazione, viewed 16 march 2025. Also relevant are the hypotheses of European Committees (assisting the European Commission) specifically created for preventive and sanctioning support related to such violations. See M. Di Florio, *Il diritto penale* cit. 9.

[41] See Consulich, *Intelligenza artificiale* cit. 262, in relation to market abuse and manipulation offenses (arts. 184-185-187 Legislative Decree 58 of 24/02/1998). Cf., regarding the issue of culpability for a strong conception of AI, Florio, *Il diritto penale* cit. 10.

In the Italian penal system, the provision under Article 113 of the Italian Penal Code has seen, especially post the now paradigmatic "ThyssenKrupp case" (Cass. Joined Chambers, 18/09/2014, n. 38343), a reevaluation in a normative-organizational perspective of the complicity institution[42]. What is the purpose of this institution in the context of the present contribution? Essentially, from the perspective of the integration between AI and IoT, between human and algorithmic activity, the potential to prevent the criminogenic degradation of automation shifts to an indeterminate number of agents involved in the complex activity[43]. Actually, it will be a functionalist approach, so-called "by role," that will impose limitations on the expansion of positions of guarantee, which, when intertwined with the factuality of negligence (*ex* Article 40.2 of the Italian Penal Code, in conjunction with Articles 43, 110, and 113), risk objectifying criminal liability beyond the already challenging concept of omission - *suitas* - (i.e., preventative omission).

Social expectations[44] of reference are suitable for delimiting the risk factors in a complex system. While they are subject to criticism for their extreme factualization of the role, they allow for the identification of which behaviors have the appropriate parameters to become typical in the context of pluralistic prevention[45] (impedimento plurisoggettivo).

Indeed, careful doctrinal analysis has emphasized the inevitable connection between information obligations regarding AI risks and the possibility of pluralistic control[46]. All of this, tied to the preventive parameter, intertwines with recent reflections on the increasing use of prevention and predictability for negligent crimes. This reflection has recently emerged in contributions focusing on the reduced human involvement in preventing negligent disasters[47].

It is necessary to delimit the field of analysis: here, we are referring to the lawful use of AI[48]. It is indeed relevant to update responsibilities according to a graduated schema: yes, the general responsible party for control, but especially those tasked with compliance for the introduction of algorithms—often predictive—entrusted with the risk assessment. The attribution schema, in fact, would not relate to the ability to "predict the foreseeable" but rather to the possibility of adjustment "according to the best science and experience" of the machine used (the ontological foundation for replacing human control obligations)[49].

Then, shifting focus to the differentiation between the concept of "strong" AI and "weak" AI[50], it is essential to remain within the context of the latter—AI as a functional tool for human activity—to delimit the space for imputational justification, thereby justifying the intervention of human control.

Indeed, the proposal involves using AI for monitoring infrastructures aimed at preventing negligent risks. This element can be readily extended, beyond the parameter of preventing negligent disasters,

[42] Without delving into the complex doctrinal and jurisprudential reconstruction of the institution, reference is made to F. Consulich, *Il concorso di persone nel reato colposo*, Torino 2023, *passim*., particularly 53ss., 141ss.
[43] A. Mangione, *Intelligenza Artificiale, attività d'impresa e diritto penale*, Torino 2024, 278ss.
[44] G. Jakobs, *Sistema dell'imputazione penale*, Napoli 2017, trad. it. L. Cornacchia, 110.
[45] Since it is capable of actualizing predictability, see Jakobs, *Sistema dell'imputazione penale* cit. 110.
[46] With specific regard to business management, see A. Mangione, *Intelligenza Artificiale, attività d'impresa e diritto penale*, Torino 2024, 288ss.
[47] Cf. Di Florio, *Il diritto penale* cit. 1-7; A. Cappellini, *Reati colposi e tecnologie dell'intelligenza artificiale*, in *Arch. pen.* 2 (2022) 4ss.
[48] L. Picotti, *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. proc.* 3 (2024) 298ss. For the considerations regarding intentionally criminogenic use, or use based on unlawful grounds, see *ivi*, 297ss.
[49] Id., *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. proc.* 3 (2024) 299. Cf. L. Fimiani, *La tecnologia nel sistema penale: dalla giustizia predittiva alle problematiche sull'utilizzo della "IA" per prevenire episodi criminosi*, in *dis. Crimen* november 18th (2024) 8ss.
[50] See *supra* footnote 15.

to any function that supports the control of human activity[51]: consider, for example, an algorithmic tool capable of assessing whether a certain activity can surpass the illicit risk, as discussed *infra* §4. In a fully automated urban society, the element of force majeure becomes even more unpredictable[52]. As appropriately pointed out, AI would thus become a new form of 'criminal model agent' on which reliance for preventing negligent crimes could be based (with the consequence of making the negligence of the person in charge of human control more lenient), so as not to sacrifice the human relevance of the conduct, while also updating the preventive potential of the technology[53].

In practice, therefore, human responsibilization for the failure to control in the event of an adverse occurrence becomes significant[54]. This requires the introduction of new categories of negligence, in order to better adapt to the control system. A proposed hypothesis for the system of imputation would be negligence in action (*culpa in agendo*), a form of negligence arising from increasing or creating the illicit risk coefficient derived from the use of AI, together with the creation of dangerous situations due to "the failure to implement a protective framework around AI operations and the failure to promptly implement security measures in response to warning signals"[55]. Alternatively, in the context of pluralistic responsibility, a true and proper negligent offense could be created, integrable through the general clause in Article 113 of the Italian Penal Code, for the mismanagement of risk—hypotheses that, as noted, are also suitable for the political transformation of offense scenarios into conduct-based offenses in relation to criminal negligence[56].

Bringing this context into the reality of prevention via surveillance, positive legislative insights become useful: indeed, the assumption of protocol-based liability derived from the AI Act, reinforced by the previously mentioned human surveillance obligation (Article 14), allows for the actualization of risk management according to individual spheres of operability[57]. If the person responsible for final control already had, inherently, a sphere of competence regarding the monitoring of the individual's activity, their level of responsibility will vary depending on the preventive scalability of the AI system, thus shifting the scope of liability to the person in charge of the maintenance or training of the AI.

This functionalist approach must be accompanied by observations concerning the space of human operability *ex ante*: indeed, organizational and control parameters do not necessarily exclude human involvement per se, but do they exclude the person? That is, is the reconstruction of criminal liability and the complex system of non-liability, the exclusion of culpability, and the acceptance of lawful risk truly compatible with a mathematically defined risk prevention logic[58]? And with the

[51] Di Florio, *Il diritto penale* cit. 8.

[52] Cappellini, *Reati colposi* cit. 11-13. This is also because the precision of the machine has been scientifically proven in contrast to the progressive "unfamiliarity with attention" of humans for tasks that are already automated.

[53] Di Florio, *Il diritto penale che verrà.* cit. 13ss.

[54] Cappellini, *Reati colposi* cit. 10-12. Furthermore, the author, *ivi*, on 14ss., emphasizes how the need to reassure the victim in the face of an adverse event is one of the reasons why human involvement is always and necessarily required, beyond the well-known impossibility of *suitas* for AI, in justifying the implementation of AI systems for the prevention of criminal risks.

[55] Consulich, *Il diritto penale* cit. 19ss., personal translation. Cf. M. Colacurci, *Quale diritto penale dell'IA?: alcune riflessioni a partire dalla proposta di regolamento dell'Unione Europea*, in *Jus* 3 (2023) 365.

[56] Consulich, *Il diritto penale* cit. 21.

[57] Mangione, *Intelligenza Artificiale* cit. 310ss.

[58] Burchard, *L'intelligenza artificiale* cit. 1921ss., discusses the concept of sociological-criminal banalization, which seeks to fit behavior patterns into predetermined schemas when verifying a crime, an even more absurd idea when applied to the dynamics of negligent crimes.

construction of the legal system as a space for will[59]? Not only the reduction of risk and the reporting of illicit activities, but also the risks related to confidentiality and criminal intent, transpose into the punitive-computational phase in a strict sense. That is, how much can the algorithmic data influence the decision when it is already safeguarded by a micro-system of precautions designed to make it as objective as possible[60]?

4.- **AI-IoT devices for crime detection and risk prevention.**

One of the main advantages of smart cities is the possibility to improve public safety using smart crime detection systems. These systems employ sensors and AI-based algorithms to predict or to identify real-time criminal activities and to promptly inform local law enforcement agencies of anomalous events. The range of cases in which these systems can be used is wide, and includes monitoring of anomalous events in crowded environments, theft and violence detection, object detection, face recognition and unauthorized access of properties.

The most common technology used for crime detection is undoubtedly video surveillance. In smart cities, video and audio surveillance can be a feature of IoT devices integrated with cameras and microphones. The technological characteristics of these devices heavily depend on the type of surveillance that is carried out. Therefore, the kind of data produced and the expected latency of the analyzed results will determine characteristics such as dimension, shape, power supply and type of communication technology of the employed devices.

In the review by Pisati et al.[61] on AI-based CCTV surveillance systems, it is pointed out that one of the main concerns of using AI techniques (e.g. deep learning) is whether the employed dataset has enough examples to train the AI model to unequivocally distinguish between normal activities and subtle anomalous activities. However, results from recent examples in the literature have shown that different combinations of datasets and algorithms have produced a high accuracy in detecting crime and anomalies, and the number of false positives is low in most cases.

The 2023 survey of Myagmar-Ochir et al.[62] shows a high level of accuracy for different video surveillance systems using edge/cloud computing and deep learning algorithms. The cases analyzed include object classification, recognition and tracking, human action detection and anomaly detection. In their work it is also mentioned the dynamic role of drones as an example of UAV in the context of smart cities. Drones-based surveillance systems can be used to search areas that are difficult to reach for humans. Moreover, drones can be useful to track moving people or objects and to monitor areas out of the reach of fixed cameras. The role of UAVs is not only limited to crime detection, but they can be employed in search and rescue operations, environmental monitoring and traffic management[63]. However, drawbacks such as short battery lifetime or weakness in harsh weather conditions may be a limiting factor for their deployment in smart cities.

A practical example of how crime prevention tools can be implemented in smart cities is the Incheon Free Economic Zone (IFEZ) case, which comprises the three Korean smart cities of Songdo, Cheongra, and Yeongjong. These cities are part of the U-City project, a large Korean smart city

[59] Possibility of error as a prerequisite for law and its function? In relation to criminal law as the protection of liberty, cf. Id., *L'intelligenza artificiale* cit. 1925ss.

[60] On the risk of unpredictability in deep learning, see Mangione, *Intelligenza Artificiale* cit. 406.

[61] R. Pisati et al., *A Profound Review of AI-Driven Crime Detection in CCTV Videos*, in 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT), India 2024, 193ss.

[62] Y. Myagmar-Ochir et al., *A Survey of Video Surveillance Systems in Smart City*, in *Electronics* 12.17 (2023) 3567.

[63] N. Dilshad et al., *Applications and Challenges in Video Surveillance via Drone: A Brief Survey*, in 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South) 2020, 728ss.

investment which was the first among developed countries to be focused on building new cities with smart control of urban infrastructures. Park et al.[64] have analyzed in their study the early results of the IFEZ's smart crime prevention service in the years 2017-2018. The three smart cities are managed by a single Integrated Operations Center that employs a video surveillance system for security services like crime detection and environmental monitoring. The data collected from the smart sensors is analyzed in real-time by an intelligent video surveillance system that is able to identify anomalous events and notify the Integrated Operations Center. To manage multiple real-time events, all the emergencies are also classified by the system with a rating based on their priority. Afterwards, the agents can make a final control and warn the competent authorities of the emergency. The smart detection tools provided by the city are in particular CCTVs cameras integrated with an abnormal sound source detection device, which are able to recognize explosions or collisions and search vehicle numbers.

The results of the analysis of Park et al. show a high rate of false alarms due to a high sensitivity of the IoT devices. This problem forced the IFEZ's smart cities to discontinue some of the AI-services of the CCTVs cameras due to an excessive workload for the agents of the Integrated Operation Center. This case study is of particular importance because it shows the consequences arising from the employment of immature technologies. The sensors were too sensitive for their scope, and the AI algorithms employed were not based on machine learning techniques. The data used was not highly specialized for smart crime prevention, and there was little effort from government agencies to create a shared dataset. Moreover, there was little interest from the private sector to invest in smart services. However, there are also many examples of successful employment of crime detection tools, and more in general smart services, in important smart cities such as London, Singapore and Helsinki[65]. For example, in Singapore, sensor cameras with face recognition software have significantly helped to achieve 322 non-consecutive days without robberies or thefts in 2018.

The success of a smart city can also be measured on whether its services are appreciated by its citizens. From this point of view, a useful dataset is the IMD Smart City Index[66]. The SCI is based on surveys that have the scope to gather information about the satisfaction of the smart city services, focusing on the structures and the technologies of the city. It includes, for example, questions about whether CCTV cameras have made residents feel safer, or whether traffic, environmental and medical digital services are well managed and accessible to the population. In addition to the already mentioned smart cities, we find leading in the index a lot of European smart cities (Zurich, Oslo, Geneva), but also Middle East (Abu Dhabi, Riyadh) and East Asian cities (Beijing, Taipei City, Seoul), while most North American cities are facing a negative trend.

In the context of healthcare, an efficient and cost-effective solution to improve digital services is to create smart IoMT networks. The integration of IoT devices and AI algorithms can allow medic personnel to remotely monitor patients and predict their health trends. Patients with chronic diseases or serious illnesses will feel safer knowing that their parameters are evaluated even when their medic is not checking them. Moreover, the data collected over time can be used by the medics to perform analysis on whether prescribed drugs are being effective or there is the need to change the treatment of the patient.

[64] M. Park et al., *Smart City Crime Prevention Services: The Incheon Free Economic Zone Case*, in *Sustainability* 12.14 (2020) 5658.
[65] J. Vodák et al., *Advanced Technologies and Their Use in Smart City Management*, in *Sustainability* 13.10 (2021) 5746.
[66] IMD Smart City Index webpage: https://www.imd.org/smart-city-observatory/home/.

In their review, Kakhi et al.[67] have pointed out that the IoMT can help to reduce some of the main struggles of medical services such as annual increase of medical cost and insufficient number of medical experts. Furthermore, IoMT also reduces the need for in-person medical visits and consequently avoids crowds in hospitals.

From a technological point of view, the main concern in developing such services is mostly connected to the power consumption of the IoT devices. As was mentioned for the IFEZ case, an appropriate choice of hardware technologies is fundamental to avoid service failure, since IoMT devices like wearables should not be heavy to carry or difficult to handle. Moreover, the integration of AI in these devices is not directly in their software, but through cloud services, so in order to guarantee real-time data analysis and avoid excessive power consumption, it is also required to implement an appropriate communication technology. The biosensors currently used in the acquisition of biomedical signals usually use short range communication technologies like Bluetooth to transmit data to gateways. Some of these devices are fitness trackers, chronic pain wearables, cancer cell detectors, smart pillboxes and smart beds[68].

Another key example of an AI-driven IoT field is the Internet of Vehicles. Smart services, such as autonomous driving and traffic insights, are powered by machine learning algorithms that analyze real-time data collected from sensors like lidars and cameras. Multiple algorithms have enabled smart on-road functions like object and lane detection, path planning, motion control and behavior prediction. Some of the collected data can also be shared in a more expanded network of vehicles and infrastructures in order to optimize traffic flow, predict anomalies and personalize the driving experience[69]. The intrinsic risk of these services, in particular for autonomous driving, should be addressed in terms of cybersecurity by implementing robust algorithms and continuous testing of the software.

A fundamental point to highlight is that the success of the IoV and IoMT, and more in general any smart city service, heavily depends on the efficacy of the hardware and software used, as well as the safety, reliability and ethical aspects of the AI algorithms and their regulation.

5.- **Security challenges in IoT-based Smart Cities.**

As shown in the Smart City Index, the performance and the development of a smart city are profoundly dependent on the feedback given by its citizens. The previously mentioned IFEZ case is an example of how a premature choice of devices and algorithms can stop the services of a smart city and reduce trust. To avoid similar situations, the development of an IoT system should also rely on trust management to assure that each layer of the IoT stack is providing a trustworthy service. Some of the goals that should be achieved are reliability in data collection and sensing, personal information preservation according to the user expectations, trustworthy processing and transmission of the data, quality of service and system security and robustness[70]. These goals extend also to trust management in AI-based applications like chatbots and facial recognition software. In particular, an AI service is perceived more trustworthy when its performance is consistent over a period of time and across

[67] K. Kakhi et al., *The internet of medical things and artificial intelligence: trends, challenges, and opportunities*, in *Biocybernetics and Biomedical Engineering* 42 (2022) 749ss.

[68] F. Al-Turjman et al., *Intelligence in the Internet of Medical Things era: A systematic review of current and future trends*, in *Computer Communications* 150 (2020) 644ss.

[69] D. Garikapati et al., *Autonomous Vehicles: Evolution of Artificial Intelligence and the Current Industry Landscape*, in *Big Data Cogn. Comput.* 8.4 (2024) 42.

[70] Z. Yan, P. Zhang, A. V. Vasilakos, *A survey on trust management for Internet of Things*, in *Journal of Network and Computer Applications* 42 (2014) 120ss.

various situations. Users will rely more on that technology if the results of their inputs are predictable and dependable[71]. Furthermore, trust of smart crime detection tools, IoMT and IoV services, heavily depends on the credibility of the institutions and private companies that build and deploy them.

Many IoT sensors continuously produce large amounts of data that in most cases contain personal information and may become security threats used for identification, localization, tracking or profiling of a user. Fortunately, most of these issues are already known threats of classical internet applications for which there are many cybersecurity solutions. However, the computational complexity and energy consumption of the traditional algorithms and encryption standards can't always be adapted to fit the resource-constrained requirements of IoT systems[72]. Security methods for smart cities also include blockchain-based IoT applications[73], biometric identification through voice, face or fingerprint recognition and AI techniques. For example, machine learning and deep learning methods can be used for network intrusion detection, but they are not usually trained specifically for IoT systems and may not have the expected performances. In fact, a current research topic is to train new AI models for intrusion detection using ad-hoc techniques and datasets for IoT networks[74].

Assembling an appropriate dataset, together with a good algorithm design, is fundamental to be able to train an efficient AI model. In some cases, as in the context of criminal justice and healthcare, datasets should also be collected by making sure that any possible bias is avoided. As mentioned by E. Ferrara[75], there are already many real-world examples of AI systems that present bias in their evaluations. In fact, as demonstrated by a study of the National Institute of Standards and Technology (NIST)[76], facial recognition technologies have been found to lead to a higher rate of false positives for people with darker skin tones. Moreover, other studies have also found some biases in the COMPAS system, an AI algorithm used in the United States criminal justice system to evaluate criminal recidivism. According to C. Engel et al.[77], the COMPAS algorithm is not only biased against certain groups of defendants, but against all kinds of defendants. Therefore, the system is more likely to suggest to keep the accused into custody than to release him. Different strategies such as pre-processing data, model selection and post-processing decisions can be employed to mitigate bias in AI systems, but they can be time-consuming, complex to use or not always effective. Moreover, since AI biases may be deriving from a vast range of problems in the dataset, mitigation techniques should be chosen with regard to specific types of biases.

In the more general context of smart cities, other less orthodox techniques such as participatory planning can be a valid solution. This method aims to generate socially responsible AI systems by engaging the community in the development of the service like it would be done when establishing parks or other public urban infrastructures. This is a way to both ensuring transparency and improving

[71] R. Yang et al., *User trust in artificial intelligence: A comprehensive conceptual framework*, in *Electronic Markets* 32.4 (2022) 2053ss.
[72] L. Cui et al., *Security and Privacy in Smart Cities: Challenges and Opportunities*, in *IEEE Access* 6 (2018) 46134ss.
[73] L. Allen Chijioke Ahakonye et al., *Tides of Blockchain in IoT Cybersecurity*, in *Sensors* 24.10 (2024) 3111.
[74] A. Qaddos et al., *A novel intrusion detection framework for optimizing IoT security*, in *Sci Rep* 14.1(2024) 21789.
[75] E. Ferrara, *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies*, in *Scientific Reports* 6.1 (2023) 21789.
[76] R. Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*; in *NIST Special Publication* 1270 (2022) 1ss.
[77] C. Engel et al., *Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism*, in *Artificial Intelligence and Law* (2024).

trust in the deployed smart services[78]. This strategy could also be implemented in the context of smart video surveillance, as numerous law enforcement agencies, such as the Chicago Police Department[79], have faced controversies due to the lack of transparency in their algorithms.

6.- **Predictive Justice: Critical Observations and Regulation Between Prevention and Commensuration.**

The issue of predictive justice is undoubtedly one of the primary testing grounds for the analysis of the intersection between AI and law: both from the perspective of the machine judge and from the perspective of the evidence derived from predictive algorithms[80].

In a context of full urban automation, however, the problem of the subtlety involved in evading the watchful and inspectorial eye of the machine, only to later be punished in light of that scrutiny, becomes even more problematic. In fact, we are witnessing a form of "technological paternalism" which renders the continued defense of the penal system as a last resort paradoxically relevant, in contrast to the rising first-line tools that are capable of supporting social defense, as they take on an increasingly prominent role in prevention[81].

While it is to be hoped that a non-catastrophic approach is maintained (i.e., one that does not adopt a Robocop-like vision of robotic policing or the absence of human qualities in investigative activities)[82], a precautionary attitude is necessary in addressing: 1) the potential abuse of tools used in the parameterization of crime detection instruments, and 2) the biases that algorithmic tools may introduce in identifying the subject to be detected and potentially punished[83].

Turning to the first point, a brief examination concerns the current application of IoT systems in urban areas facing problems not directly attributable to human "conduct": for instance, software used in "urban criminology" (e.g., in degraded areas with poor lighting) capable of identifying hotspots conducive to criminal activity (such as drug trafficking, assaults on persons). One such example is Risk Terrain Modeling (RTM) used in the United States and the United Kingdom, via the "PredPol" software, developed by researchers at the University of California in collaboration with local police forces. In Italy, the "X-Law" software, used by the Naples Police, is based on a database of police reports related to high-risk areas and associated crimes[84].

Another type of preventive tool falls within the category of "crime linking," which relies on a database of criminal subjects and their serial offenses to predict when they might commit new crimes (e.g., Keycrime, developed by the Milan Police, Precobs in Germany, H.a.r.t. in the UK). These tools are used not only to predict when the same type of crime will occur in similar locations but also to reconstruct the criminal career of a subject under investigation[85].

---

[78] G. Falco, *Participatory AI: Reducing AI Bias and Developing Socially Responsible AI in Smart Cities*, IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 2019.

[79] J. Saunders et al., *Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot*, in *Journal of Experimental Criminology* 12.3 (2016) 347ss.

[80] Basile, *Intelligenza* cit. 13ss., 16 ss.

[81] Burchard, *L'intelligenza artificiale* cit. 1926-1928, and regarding technical prevention, highlighting the reflections of Hassemer and Hilgendorf on this point.

[82] Cf. Basile, *Intelligenza artificiale* cit. 9ss.

[83] Burchard, *L'intelligenza artificiale* cit. 1923-1925. It is noteworthy that, in addition to having a tendency towards the evaluation of risk *contra reo*, the problem of *bias in, bias out* can also lead (with an abuse of the *pro reo* principle) to a cleansing of criminal liability considering the social qualities of the investigated individual, with evident risks concerning the area of white-collar crimes.

[84] Basile, *Intelligenza artificiale* cit. 11ss.

[85] Id., *Intelligenza artificiale* cit. 13ss.

Turning to positive law, it must be noted that certain practices are, in fact, prohibited: this includes social scoring systems, which involve analyzing individual behavior to assess reliability or to characterize a person's criminal personality. Furthermore, the use of real-time biometric identification systems would be prohibited unless in the context of "research activities related to a serious crime" (Article 83.1 TFEU)[86].

Predictive policing and predictive justice systems are analyzed and regulated under the AI Act[87]. Particular criticism is directed at tools that evaluate human personality, feelings, and emotions, as these could function as a form of modern "lie detector." As a result, personal-based profiling tools are moved from the category of high-risk practices to prohibited practices, as they are likely to violate human dignity, the presumption of innocence, and non-discrimination[88]. Beyond this, the regulation maintains the legality of these tools where they serve investigative rather than preventive functions, including suspect-based systems and place-based systems[89], placing them in the category of high-risk systems subject to human oversight.

As rightly pointed out, despite compatibility with the principles of criminal law as they intersect with human rights, there remains a problematic instrumental view of all these tools within the system of preventive measures, which, even today, is already subject to critical attention for being overly instrumental and operating outside the safeguards of the presumption of innocence[90].

Turning to the punitive aspect, it should be noted that the machine-judge directive has been met with numerous concerns, notably due to the famous and widely discussed COMPASS case[91]. Notwithstanding that judges themselves may be suspicious of being bound to automated decisions, as these could be detrimental to their inherent discretion and interpretative freedom—freedoms already well-protected by the principles governing the areas of law they handle—concern should focus on how data obtained from such tools inform the qualification of elements of proof under the scrutiny of the judge[92]. Algorithmic opacity should be addressed through explanatory systems that clarify how particular conclusions are reached, especially where the possibility of obtaining penal-relevant information arises from multiple fronts of daily societal use[93].

Indeed, how can the presence of excuses, fortuitous cases, causal interruptions, lack of proper organization, or other factors preventing criminal liability be raised if the reconstruction of the system of liability is based on subjective and objective elements (often not interacting) within the theory of

[86] Reference is made to M. Colacurci, *Quale diritto penale dell'IA: alcune riflessioni a partire dalla proposta di regolamento dell'Unione Europea*, in *Jus* 3 (2023) 366ss., for the reconstruction of the legislative process concerning the issue of real-time identification and the problem of its subordination to judicial authorization.

[87] Cf. Id., *Quale diritto penale dell'IA?* cit. 369-371; E. Pietrocarlo, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, in *Leg. pen.* september 16th (2024) *passim.*

[88] Ead., *La predictive policing nel regolamento europeo sull'intelligenza artificiale* cit. 19ss.

[89] Ead., *La predictive policing nel regolamento europeo sull'intelligenza artificiale* cit. 20-23.

[90] Ead, *La predictive policing nel regolamento europeo sull'intelligenza artificiale* cit. 30ss. Cf. Palazzo, Bartoli, *Corso di diritto penale* cit. 619ss.; G. Fiandaca, E. Musco, *Diritto penale. Parte Generale*, Bologna 2019, 929ss. See also Colacurci, *Quale diritto penale dell'IA?* cit. 371-375, for considerations regarding the impact on fundamental rights.

[91] Cfr., *ex multis* M. Di Florio, Calculate criminal law? *Criticità nell'uso degli algoritmi di pericolosità sociale*, in *Leg. pen.* 1 (2023) 4, 12-14.

[92] Di Florio, *Calculate criminal law?* cit. 9ss.

[93] Id., *Calculate criminal law?* cit. 17ss.

the offense?[94] The risk is that individuals may be tied to events[95] and rendered indefensible due to continuous surveillance.

Italian legislative intervention (draft bill 1146/2024) adopts an oppositional stance regarding the use of AI systems in judicial decision-making. After clarifying their instrumental use for organizing and simplifying judicial work, as well as for research in databases (Article 14.1), the bill opposes the use of AI systems by judges for interpreting the law, evaluating facts and evidence, or issuing decisions (Article 14.2)[96].

Currently, the use of AI for the repression of cybercrime has gained particular success in functions beyond preventive and investigative measures, especially in the fight against money laundering and terrorism financing[97] (without venturing into individual profiling but focusing on criminal instruments in the context). It would be anachronistic to advocate for the abandonment of the integration between criminal law and new technologies, as the limits placed on punitive measures are grounded in motivational risks[98] and equality of treatment[99].

In terms of updating, should we not reach a definitive closure regarding the use of algorithms in judicial decisions, their role would remain in the commensurability phase (Articles 132 and 133 Italian Penal Code). There are existing experiments for assessing proportionality and adequacy in the qualification and quantification of penalties (e.g., the Ex-Aequo algorithm)[100], where algorithmic assistance serves to compare similar criminal episodes and previous decisions. Beyond objective parameters, algorithms of this nature, when trained, could allow for a more subjective assessment of the characteristics of the criminal act in light of the specific circumstances[101]. The hope is that, in an effort to provide investigators with greater access to evidence through AI systems, greater care will be taken in assessing the factual context of the incidents and the "psychological pressure" that accompanies continuous human observation[102].

Ultimately, the integration of criminal law with the full digitalization of society may open up new spaces for the realization of social protection needs, with evident consequences for investigative measures, and the enhancement of prevention in the face of the risk of wrongful imputations based on chance. Human oversight remains the only safeguard, both in the preventive and punitive phases, and serves as a countermeasure to the growing skepticism surrounding the advancement of AI. In a transformative perspective, the development of a "strong" concept of AI would allow for the creation of new spaces of liability for machine subjectivity, effectively eliminating the risk of imputing liability for omissions that, in conjunction with liability for negligence crimes, often lead to the risk of objective liability[103].

---

[94] Moreover, it is worth noting the risk of the imprecise ability to integrate the rule of judgment "beyond any reasonable doubt" as stated in Article 533.1, of the Italian Criminal Procedure Code see Basile, *Intelligenza artificiale* cit. 16.

[95] With poetic expression see M. Sgalambro, *Del delitto*, Milano 2009, 121. «Se il delitto radicato nel nostro stesso essere non diventa un vero oggetto di conoscenza, quest'ultima non sarà mai in grado di consegnare alla nostra compassione né l'assassino né la vittima».

[96] Romano, *Il DDL in materia di IA* cit. 412ss.

[97] Di Vizio, *Prevenzione e investigazioni* cit. 54ss.

[98] G. Tuzet, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in *MediaLaws* march 16th (2020) 5-8. Cf. Ubertis, *Intelligenza artificiale* cit. 78ss.

[99] Id., *L'algoritmo* cit. 8-10.

[100] F. Coppola, *Commisurazione della pena e intelligenza artificiale: una ipotesi di lavoro con l'algoritmo Ex-Aequo*, in *Arch. pen*. 2 (2023) 20 ss.

[101] Id., *Commisurazione della pena* cit. 22.

[102] See Consulich, *Il diritto penale* cit. 1-4.

[103] Consulich, *Errare commune est.* cit. 24ss.

Abstract.- L'intersezione tra intelligenza artificiale (IA), Internet of Things (IoT) e diritto penale apre nuove sfide in materia di responsabilità, prevenzione del rischio e tutela dei diritti fondamentali. Nel presente contributo vengono analizzate le implicazioni normative delle principali tecnologie AI-IoT, con particolare attenzione al diritto penale del lavoro, alla responsabilità medica e ai reati colposi. Inoltre, vengono esaminati il ruolo della giustizia predittiva e i rischi connessi all'automazione delle decisioni nel contesto delle Smart Cities, sottolineando la necessità di un controllo umano significativo e di un adeguato quadro regolatorio che contrasti le emergenti problematiche di sicurezza.

The intersection of artificial intelligence (AI), the Internet of Things (IoT), and criminal law raises relevant challenges related to liability, risk prevention, and the protection of fundamental rights. In this paper, the regulatory implications of the main AI-IoT technologies are discussed, with a focus on labor criminal law, medical liability, and negligent offenses. The role of predictive justice and the risks associated with automated decision-making in the context of Smart Cities are also examined, emphasizing the need for meaningful human oversight and a proportionate regulatory framework to address novel security challenges.