# Artificial Intelligence and Crime: Challenges of Criminal Liability in the Age of Algorithms

**Hamouti Nadia[1], El Bakouhi Safae[2]**

---

**Science Step Journal / SSJ**

**2026/Volume 4 - Issue 12**

**To cite this article:** Hamouti, N. & El Bakouhi, S. (2026). Artificial Intelligence and Crime: Challenges of Criminal Liability in the Age of Algorithms. Science Step Journal, 4(12). ISSN: 3009-500X.
https://doi.org/10.5281/zenodo.20090594

---

## Abstract

Artificial intelligence (AI) is increasingly playing a vital role in the criminal law domain, both as a means to prevent and fight criminal offenses and as a means that gives rise to new forms of criminal offenses. Therefore, the main objective of this article is to analyse the role of artificial intelligence in the prevention and fight against criminal offenses, as well as the challenges it poses to criminal law at the national and international levels. In this context, it is necessary to refer to the role of artificial intelligence in surveillance, criminal investigation, cybersecurity, and criminal justice, while focusing on the risks associated with its use for criminal purposes. Regarding the methodology used in this research paper, it is necessary to refer to the fact that it is based on an analytical and critical approach to the subject matter, focusing on the study of legislative frameworks at the national and international levels, as well as reports and cases related to cybercrime. This methodology enables the evaluation of the sufficiency of the criminal law rules in the context of the criminal offenses related to artificial intelligence, in particular concerning criminal liability and the protection of fundamental freedoms. This article shows that, in spite of the opportunities offered by AI to improve the efficiency of the criminal justice system, the lack of a harmonized legal framework generates legal uncertainty. It highlights the need to adapt criminal law in order to ensure the effective prosecution of AI-related crimes while guaranteeing the fundamental principles of legality, proportionality, and the protection of human rights.

**Keywords:** Artificial intelligence; criminal law; cybercrime; criminal liability.

[1] Professor at University Sidi Mohammed Ben Abdellah, Fez, Morocco. Nadia.hamouti@usmba.ac.ma
[2] PhD student at University Sidi Mohammed Ben Abdellah, Fez, Morocco. Safae.elbakouhi@usmba.ac.ma

**Introduction:**

Artificial intelligence (AI) is one of the most powerful and promising technologies of the 21st century. In just a few decades, it has transformed many sectors, from healthcare to finance, education, and security (Floridi, 2019, pp. 3-7). In the field of crime, AI plays an ambivalent role: it can be used to prevent and solve crimes, but it can also become a tool for criminals (Delmas-Marty, 2010, pp. 45-52).

Artificial intelligence entities have become an unavoidable reality and are performing actions that were previously reserved for human intelligence, as artificial intelligence is one of the modern fields of science and knowledge that is undergoing rapid development. It is a branch of computer science based on the science of engineering intelligent mechanisms, i.e., the science of creating devices and computer programmes capable of thinking in the same way as the human brain, learning as you learn, deciding as you decide, and behaving as humans behave.

Crimes related to artificial intelligence are considered crimes of the near future, except that some of them have already begun, as technological development has contributed to the emergence of many of these crimes.

It is now certain that artificial intelligence plays a more important and profound role in various branches of science, particularly in the field of crime fighting (Brundage, 2018, p :12-18). Indeed, the police can use artificial intelligence to analyse databases of reports in order to direct patrols to areas that need to be secured, and criminal behaviour now makes use of information networks and modern technologies, making it easier to escape punishment, as many crimes are committed at an international level.

Faced with this dual nature of artificial intelligence, which presents itself both as a tool of progress and as a potential source of risks, it becomes essential to examine its implications for society. In this context, a central question arises: how does the use of artificial intelligence in criminal contexts create both opportunities and risks for society.

Regarding the methodology used in this research, it is based on an analytical and critical approach, focusing on the examination of national and international legal frameworks, as well as relevant reports and case studies related to cybercrime. This approach allows for an assessment of the adequacy of existing criminal law rules in addressing AI-related offenses, particularly in relation to criminal liability and the protection of fundamental rights.

This reflection will lead us to explore not only the positive applications of AI in the fight against crime, but also the dangers it can pose if misused for malicious purposes.

This requires us to examine artificial intelligence as a tool for fighting crime **in Part I** and the risks associated with the use of artificial intelligence in crime **in Part II**.

**Part I - Artificial intelligence as a tool for crime prevention and law enforcement**

From this perspective, artificial intelligence is emerging as a key tool for modernising the work of public authorities. It is primarily used in mechanisms for monitoring and preventing crime, enabling better anticipation of criminal behaviour and more efficient allocation of security resources.

**Chapter 1 - Artificial intelligence in the service of criminal surveillance and crime prevention:**

AI is a tool increasingly used by authorities to improve the effectiveness of crime surveillance and prevention. Due to technologies such as facial recognition, predictive algorithms and autonomous drones, it is now possible to identify suspicious behaviour before it escalates into criminal acts (Binns, 2018, p:1-14). For example, facial recognition software can analyse surveillance videos to quickly identify wanted individuals (Lyon, 2001, p:21-30). Similarly, some crime prediction systems, powered by historical data, are able to predict where and when a crime is likely to occur, allowing law enforcement agencies to anticipate and better target their interventions (Hughes, 2019, p: 4-6). Even though this may pose some privacy concerns, this approach has already proven to be effective in some cities, especially in the United States, in the reduction of some types of crime.

While AI is important in the physical world for the prevention of crime, it is equally important in the digital world where crime is also on the rise.

**Chapter 2 - The role of artificial intelligence in the fight against cybercrime and digital economic crime:**

AI also plays a crucial role in cybersecurity. Cyberattacks (W. Brenner, 2010, p:63-75), whether hacking, ransomware or DDoS (denial of service) attacks (ENISA, 2020, p:15-22), are becoming increasingly sophisticated. AI systems are capable of detecting abnormal behaviour or hacking attempts in real time by analysing billions of pieces of data and identifying patterns invisible to the human eye. Due to the use of machine learning, these systems can not only anticipate attacks and respond at once, but they can do so in real time. In this way, AI not only helps to protect sensitive information belonging to businesses and government agencies, but also contributes to the fight against online crime, which is a growing threat in our hyperconnected world.

In this context, we can address the issue of economic crime in the virtual world. This is a crime of a physical nature, represented by any illegal behaviour involving the use of electronic devices in a

way that allows the criminal to obtain material or moral benefits, while imposing a corresponding loss on the victim. The objective of these crimes is often hacking in order to steal or destroy the information contained in the devices and then extort money from people using this information, which necessitates a solid wall to protect companies from these risks that threaten them and their activities.

- Credit card number theft offences:

One type of computer crime is the theft of electronic credit cards (FBI, 2021, p:18-24), as many countries face the problem of illegal use of electronic credit cards, whether by the cardholder or by third parties (Roscini, 2016, p:6-12).

-Cyberterrorism:

This is the most worrying criminal phenomenon to have emerged with the spread of malware and the possibility for terrorists to use the internet to destroy and sow chaos (Brundage, 2018, p:31-37). For example, terrorists can place temporary electronic bombs in several locations in a city, link them together and send electronic codes to detonate these bombs simultaneously, without the need to plant explosive devices or booby-trap cars, and these electronic bombs can cause damage to the environment. They can also alter the composition of medicines by hacking into pharmaceutical factories, causing the deaths of many innocent people, and they can also hack into the electricity grid, destroy it or deactivate smart meters, increase or decrease their consumption, and alter natural gas levels, causing the destruction of safety valves, which can lead to huge explosions and severe burns.

-The use of technology to facilitate human trafficking:

Human trafficking is one of the forms of transnational organised crime, as human trafficking in its various forms has become a crime that uses computers and the internet, providing traffickers and smugglers with unprecedented opportunities to conduct business related to human trafficking (UNODC, 2020, p:52-59).

Perpetrators use websites to attract as many people and children as possible from around the world, offering site members or visitors all kinds of material and moral incentives, tricks, means of deception, etc., and promising them lucrative jobs. Traffickers often create websites in the countries of origin and in the languages of the victims who are at risk of being trafficked (Brenner, 2010, p:141-146).

A distinction must be made between traffickers who create the websites themselves and then exploit the victims they recruit, and operators who are paid by traffickers to use the websites and thus become their partners, playing a key role in online human trafficking because they have the technical knowledge to create the websites and conceal electronic traces from the police.

**Chapter 3 - Artificial intelligence in criminal investigation and digital evidence management:**

Artificial intelligence can also facilitate the analysis of large amounts of data in criminal investigations. Modern investigations generate a considerable volume of evidence: documents, testimonies, videos, bank statements, etc. AI can help investigators sort, analyse and link this information more quickly than a human being (Kerr, 2005, p:281-289). For example, semantic analysis software can identify inconsistencies in witness statements or link disparate pieces of information that would otherwise have gone unnoticed. This enables law enforcement agencies to solve cases more efficiently and deliver justice more quickly (Brenner, 2010, p:201-210).

We can also talk about proactive policing, which means deterring criminal activity through proactive policing based on data analysis and evidence. One of the most important measures in this regard is the adoption of computer storage systems by security agencies, which will be a key factor in preventing and reducing modern crime, given that the amount of data circulating with technological development is increasing exponentially, and computer storage will solve the problem of storage and allow security networks to be linked together to facilitate work on crimes (Brenner, 2010, p:201-210).

There is also digital policing, which involves developing police services to become more technologically savvy in everything they do to take advantage of the abundance of digital evidence that can be found in CCTV footage, emails and telephone recordings, making it necessary to have legal links between different organisations to easily provide digital evidence.

Modern technologies must be exploited and developed using artificial intelligence techniques to become more effective in gathering information on criminals and analysing data in order to use this information to aid rapid and effective decision-making.

There is also digital forensic investigation: this is a science that combines law and computer science to collect and analyse data from activities, networks, wireless communications, and storage media, to collect evidence in a form that can be adopted as admissible evidence in court and in a manner that helps to achieve the objective of the investigation.

One of the unique features of digital investigation is that it does not require the presence of the perpetrator of the crime, which is found in common cases such as monitoring compliance with security laws and regulations in a given organisation to ensure compliance with digital security rules, where digital records in IT departments can be used as evidence of compliance with these standards, and digital investigation can help by examining the vulnerabilities of these systems (European Commission, 2019, p:12-18).

However, the growing use of artificial intelligence cannot be considered solely from the perspective of its benefits. It also creates new criminal risks that need to be examined.

## Part II - Artificial intelligence as a factor in the renewal of forms of crime and criminal risks

Artificial intelligence cannot be viewed solely as a tool for security and criminal justice. Its increasing accessibility and automation capabilities also make it a preferred means of committing offences, paving the way for new forms of crime that are particularly complex to address through criminal law.

### Chapter 1 - The criminal exploitation of artificial intelligence: new ways of committing offences

While AI offers powerful tools for fighting crime, it can also be used for criminal purposes. One of the major dangers lies in the use of AI to create more sophisticated cyberattacks. For example, criminals can use algorithms to automate large-scale cyberattacks, such as the theft of personal data or the spread of malware. Deepfakes, videos or audio recordings falsified by AI, are also a formidable tool for blackmail, manipulation of public opinion and fraud. These technologies make it possible to manipulate the appearance of reality, which can destabilise victims or distort investigations (Citron, 2019, p:1761-1770).

- Bots and artificial intelligence used for personal data trafficking

Another area where criminals use AI technologies is in the trafficking of personal data. AI-powered bots can be used to collect personal data on a massive scale, scanning public databases, social networks, or even illegally accessing databases belonging to companies or government institutions. AI enables this data to be processed and analysed quickly, facilitating the creation of detailed profiles of potential victims for targeted scams or social engineering attacks (ENISA, 2020, p:33-38).

This data can then be resold on the dark web, where it fuels various illegal markets. AI also allows criminals to sort and classify this information so that it can be used more effectively in large-scale attacks. For example, a hacker can use AI to predict user behaviour patterns and design phishing attacks that are more tailored to the specific needs of each target.

### Chapter 2 - The automation of criminal offences through artificial intelligence

Another worrying aspect of AI is its ability to automate criminal activities. For example, AI programmes can be used to carry out cyber attacks without human intervention, making it more difficult for authorities to identify those responsible. Criminals could also use AI to design

increasingly sophisticated hacking software, making cybersecurity increasingly fragile. The self-learning ability of AI makes these attacks more adaptive and difficult to counter.

**-Automated cyberattacks**

One of the most common and worrying uses of AI by criminals is in **cybercrime**. AI enables hackers to launch much more sophisticated and autonomous attacks. For example, **ransomware** (ENISA, 2020, p:33-38), which is malware designed to block access to data or a computer system in exchange for a ransom, can now be powered by AI algorithms. This kind of software is able to learn from the environment in order to evade the security systems put in place (McKinsey & Company, 2020, p:64-69).

As such, it is extremely difficult for the authorities to track the activities of such cybercriminals. Furthermore, phishing attacks as well as identity theft attacks are being driven further by AI-based technologies. AI algorithms are able to analyse vast amounts of personal data in order to create extremely convincing phishing messages. AI is also able to assist in the automation of these types of cyberattacks (Tirole, 2020, p:3-4). For example, AI is able to automate the sending out of personalized phishing messages to thousands of targets at once. There is a higher possibility that the targets will reply to the messages due to the fact that they are more convincing and difficult to identify as phishing messages.

**Chapter 3 - The security abuses of artificial intelligence: mass surveillance and violations of fundamental freedoms**

Another major risk associated with the use of AI is its ability to enhance surveillance systems, which are normally employed in an invasive manner. Some authoritarian regimes have been able to use AI systems to monitor their populations in real-time and even identify "suspicious" individuals and suppress "deviant" behaviour. At this point, the use of AI is no longer for the protection of society, but rather for social control. Therefore, if malicious entities such as governments or companies are able to get their hands on this technology, human freedoms could be compromised and a surveillance society could emerge (Cour européenne des droits de l'homme, 2021, p:323–336).

**Conclusion:**

Artificial intelligence, while providing many advantages in the fight against crime, also provides complex challenges. Artificial intelligence can be used to improve security, help in investigations, and protect digital infrastructure, but it also provides serious risks if used for criminal purposes or mass surveillance. It is important to create effective and clear rules to govern its use and ensure that individual liberties are protected. Finally, society must continue to evaluate the ethical

implications of this technology and how it can be used for the greater good, while minimizing the potential for abuse.

There are several recommendations for AI and crime, including the regulation of AI, where the issue of AI regulation is of utmost importance. While this technology provides promising resources for security, it must also be governed by strict regulations to ensure that it is not used for criminal purposes. Specialized legislation must be created to regulate the use of surveillance technology, particularly facial recognition software, and predictive algorithms in criminal investigations. It is also important that citizens are given assurances about the protection of their personal data and the systems used by the government.

In addition, an ethical dilemma is also raised in the context of security and individual liberties. The application of technology in the surveillance of individuals or in the prediction of criminal behaviour prior to the commission of a crime raises an ethical dilemma in the context of preventive justice. Can an individual be punished for a crime that has not been committed yet? To what extent can an individual's privacy be violated in order to guarantee his or her security?

Moreover, in the context of the malicious application of AI, an ethical dilemma is raised in the context of liability. Who is responsible in cases where a crime is committed through the use of AI? Is it the developer of the algorithm or the user of the technology? The legislation has yet to keep up with this reality, and this makes the task of the judicial authorities even more difficult in prosecuting individuals who apply this advanced technology in committing crimes.

## References


- Binns, R. (2018). Human judgment in algorithmic loops: Individual justice and automated decision-making. *AI & Society, 33*(4), 469–472. https://doi.org/10.1007/s00146-018-0822-1
- Brenner, S. W. (2010). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Beard, S., Belfield, H., Farquhar, S., Lyle, C., … Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv. https://arxiv.org/abs/1802.07228
- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0ZJ4J
- Cour européenne des droits de l'homme. (2021). *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). https://hudoc.echr.coe.int
- Delmas-Marty, M. (2010). *Libertés et sûreté dans un monde dangereux*. Seuil.
- European Commission. (2019). *Ethics guidelines for trustworthy artificial intelligence*. Publications Office of the European Union. https://digital-strategy.ec.europa.eu
- European Union Agency for Cybersecurity (ENISA). (2020). *Artificial intelligence and cybersecurity*. Publications Office of the European Union. https://www.enisa.europa.eu
- Federal Bureau of Investigation. (2021). *The use of artificial intelligence in cybercrime investigation: Challenges and opportunities*. U.S. Department of Justice.
- Floridi, L. (2019). *The ethics of artificial intelligence*. Oxford University Press. https://doi.org/10.1093/oso/9780198812849.001.0001
- Hughes, D. (2019). Predictive policing: How AI is changing law enforcement. *The Crime Report*. https://thecrimereport.org
- Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Columbia Law Review, 105*(1), 279–318.
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.
- McKinsey & Company. (2020). *Artificial intelligence: The next digital frontier?* McKinsey Global Institute. https://www.mckinsey.com
- O'Flaherty, K. (2020). Deepfakes, AI, and the new frontier of cybercrime. *Forbes*. https://www.forbes.com
- Roscini, M. (2016). Cyber operations and the use of force in international law. *Oxford Journal of Legal Studies, 36*(1), 1–36. https://doi.org/10.1093/ojls/gqv028
- Tirole, J. (2020). Regulating artificial intelligence. *Journal of European Competition Law & Practice, 11*(6), 1–9. https://doi.org/10.1093/jeclap/lpaa030
- United Nations Office on Drugs and Crime. (2020). *Global report on trafficking in persons*. United Nations. https://www.unodc.org