

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

**CRIMINAL LIABILITY ARISING FROM THE USE OF ARTIFICIAL
INTELLIGENCE**

Hellalbi kheira ^{1*}, Bensalem mokhtar ²

¹ University Center- Aflou , Legal and Economic studies laboratory(Algeria),
k.hellalbi@cu-aflou.edu.dz

² University Center- Aflou, Legal and Economic studies laboratory (Algeria),
m.bensalem@cu-aflou.edu.dz

Date of send: 02/12/2024	date of acceptance: 01/01/2025	Date of Publication: 01/03/2025
--------------------------	--------------------------------	---------------------------------

***Corresponding author**

Abstract :

This study explores the intricate relationship between artificial intelligence (AI) and criminal liability, addressing the legal and ethical challenges posed by AI technologies. It examines AI-related crimes within Algerian and international legal contexts, emphasizing the roles of creators, users, and regulatory bodies. Through a descriptive-analytical approach, it evaluates existing legislation and advocates for legal evolution to keep pace with technological advancements. The study underscores the need to balance innovation with ethical considerations, offering recommendations for legal reforms and international cooperation. Ultimately, it seeks to inform policymakers and stakeholders about the necessity of adapting legal frameworks to ensure justice in the digital era.

Keywords: Artificial Intelligence (AI); Criminal Liability; Legal Frameworks; International Cooperation.

Introduction

The advent of artificial intelligence (AI) marks a transformative era in the annals of human technological advancement, heralding unprecedented opportunities and challenges. As AI systems become increasingly integrated into various sectors of society—ranging from healthcare and finance to transportation and security—their influence on daily life is undeniable. However, this rapid integration also brings to the fore complex legal and ethical dilemmas, particularly in the realm of criminal liability. The crux of the issue lies in the unique nature of AI, characterized by its autonomy, complexity, and potential for misuse, raising pivotal questions about accountability, responsibility, and governance.

This study embarks on an exploratory journey into the intricate landscape of criminal liability as it pertains to the use of AI. It delves into the heart of how existing legal frameworks grapple with crimes facilitated by or directly involving AI technologies, shedding light on the novel challenges these crimes present. Given the global reach and impact of AI, the focus will extend beyond any single jurisdiction, incorporating a special emphasis on Algerian law alongside international legal standards, to provide a comprehensive understanding of the current legal landscape and the international efforts to address these challenges.

The objective of this article is twofold. First, it aims to elucidate the complex nature of AI crimes, characterized by their sophisticated and often unprecedented modalities, which traditional legal paradigms may find challenging to address. Second, it seeks to highlight the imperative for legal systems worldwide to evolve and adapt, ensuring that they remain effective in the face of rapid technological advancements. Through this exploration, the article contributes to the ongoing discourse among policymakers, legal practitioners, and technologists, offering

insights and recommendations that aspire to harmonize the innovative potential of AI with the foundational principles of justice and accountability.

By traversing the legal and ethical landscape of AI criminal liability, this article seeks to provide a solid foundation for understanding the complexities at hand and charting a path forward. It underscores the urgency of legal reforms, the value of international collaboration, and the necessity of embedding ethical considerations into the fabric of AI development and regulation. Through this comprehensive exploration, the article contributes to shaping a future where the immense potential of AI can be harnessed responsibly, ensuring its alignment with the principles of equity, justice, and human dignity.

Employing a descriptive-analytical methodology, this study meticulously examines the multifaceted dimensions of AI-related criminal activities, the roles and responsibilities of various stakeholders (including creators, users, and regulatory bodies), and the adequacy of existing legal instruments. This approach not only facilitates a thorough investigation of the nuanced issues at play but also lays the groundwork for identifying and proposing solutions to bridge the gaps in current legal frameworks.

The study problem revolves around the increasingly complex landscape of AI-related criminal activities, necessitating a comprehensive understanding of legal frameworks and the roles of stakeholders. This involves meticulous examination through a descriptive-analytical methodology. By scrutinizing the multifaceted dimensions of AI-related crimes and stakeholders' roles, the study aims to identify deficiencies in existing legal instruments and propose solutions to bridge these gaps.

In line with this, the main questions guiding the study are centered on:

- How do the roles and responsibilities of creators, users, and regulatory bodies contribute to addressing AI-related criminal activities?
- To what extent are current legal frameworks, both at the national and international levels, adequate in effectively addressing the challenges posed by AI-related crimes?
- What solutions can be proposed to enhance regulatory measures and improve accountability in preventing AI-related criminal activities?

To address these questions, we've organized the study into three interconnected sections:

- **Section 1: Defining Key Terms and Concepts**
- **Section 2: Legal Framework and Sanctions for AI Crimes**
- **Section 3: Challenges and Perspectives in Addressing AI-Related Criminal Activities**

SECTION 1: DEFINING KEY TERMS AND CONCEPTS

Subsection 1: AI Crimes

Artificial Intelligence (AI) crimes represent a rapidly evolving category of illegal activities that are significantly impacting the legal landscape and societal norms. As AI technologies continue to advance and permeate various sectors of the economy and everyday life, they bring forth innovative capabilities that, while beneficial in many respects, also open new avenues for criminal misuse. These activities not only challenge existing legal frameworks but also raise profound ethical questions about the role of technology in modern society.

Paragraph 1: Definition of AI Crimes

AI crimes encompass a broad spectrum of offenses where AI systems play a central role, either as tools wielded by perpetrators or as targets of malicious activities. This definition captures a wide array of illegal acts, from sophisticated cyberattacks designed to compromise security systems to the manipulation of digital content for malicious purposes. (Scherer, 2016, p. 23)

The utilization of AI in these contexts offers a dual-edged sword: it enhances efficiency and capabilities in both legitimate and illicit applications, underscoring the need for a nuanced understanding of AI's impact on criminal behavior. (Casey et al., 2019, p. 65)

AI technologies, by their nature, introduce complexities in determining culpability due to their ability to learn and make decisions independently of human input. This autonomy complicates the traditional legal concepts of intent and responsibility, as AI systems can potentially take actions that were unforeseen or unintended by their creators or users. As such, the legal system faces the challenge of adapting to a landscape where actions are increasingly mediated by algorithms.

1. Deepfakes and Digital Manipulation

Deepfakes represent a particularly insidious use of AI, where the technology's ability to create hyper-realistic audiovisual content can be exploited for fraud, defamation, and misinformation. The implications of this technology are far-reaching, affecting not only individual reputations but also public trust and the integrity of democratic processes. (United Nations Interregional Crime and Justice Research Institute [UNICRI], 2021)

As deepfake technology becomes more accessible and sophisticated, the potential for harm escalates, necessitating legal responses that balance the protection of individuals and society with the preservation of free expression.

2. Automated Hacking and Cybersecurity Threats

Automated hacking tools powered by AI represent a significant escalation in the cybersecurity arms race. These tools can analyze vast amounts of data to identify vulnerabilities at speeds and scales that human hackers cannot match.

The proliferation of AI-driven hacking tools raises critical concerns about the security of personal, corporate, and governmental digital assets, highlighting the urgent need for legal and technical safeguards that can evolve in response to these threats.

3. Financial Fraud and Economic Crimes

The application of AI in financial fraud introduces a level of complexity and scale previously unattainable. AI algorithms can execute fraudulent transactions, manipulate markets, or engage in identity theft with alarming speed and efficiency. These activities not only result in economic losses but also undermine the integrity of financial systems and erode public trust in these institutions. (Casey et al., 2019, p. 65)

Addressing AI-driven financial crimes requires a concerted effort from regulators, financial institutions, and technology developers to implement robust detection and prevention mechanisms.

Paragraph 2: Legal and Ethical Considerations

The emergence of AI crimes necessitates a reevaluation of legal frameworks and ethical guidelines to address the unique challenges they present. This includes considering the liability of AI creators and users, the role of regulatory bodies in overseeing AI development and deployment, and the international dimensions of AI crimes that transcend national borders. Moreover, ethical considerations must inform the development and application of AI technologies to ensure they serve the public good while minimizing harm.

Algeria has a law (Nr 18-07, dated 10 June 2018) focused on the protection of personal data during its processing, which is crucial in the context of AI and crime. This law outlines the conditions for collecting, recording, and processing personal data, aiming to protect individuals' rights. (CMS Legal, 2021)

However, as of February 2021, the enforcement authority for this law, the National Authority for the Protection of Personal Data, was not yet established. The law anticipates various sanctions for non-compliance, including both administrative fines and criminal penalties, emphasizing the importance of data security and proper handling.

AI crimes represent a complex and evolving challenge that requires a multifaceted response from legal, technological, and ethical perspectives. (European Commission, 2020) As AI continues to advance, so too must our strategies for understanding, preventing, and prosecuting the illegal activities it

facilitates. This ongoing process will require collaboration across disciplines and jurisdictions to ensure that the benefits of AI are realized while its potential for misuse is mitigated.

Subsection 2: Parties and Institutions in AI Criminal Liability

The attribution of liability in the context of AI crimes requires a comprehensive understanding of the diverse ecosystem of actors involved. This ecosystem is not limited to those who create or use AI technologies; it extends to those who regulate, oversee, and are impacted by these systems. The multifaceted nature of AI crimes demands a multidisciplinary approach to legal and ethical governance, implicating a broad spectrum of stakeholders in the pursuit of justice and accountability.

Paragraph 1: Roles and Responsibilities

1. Ethicists and Academics:

Beyond the creators, users, and regulators, ethicists and academics play a crucial role in shaping the discourse around AI and criminal liability. Their research and analysis contribute to the development of ethical guidelines and best practices for AI use, informing policy and legal reforms.

2. Victims of AI Crimes:

The perspective of victims—individuals or entities adversely affected by AI crimes—must also be considered in the attribution of liability. Their experiences highlight the tangible harms wrought by AI crimes, underscoring the need for robust legal protections and remedies. (Casey et al., 2019, p. 54)

3. AI Systems as Legal Entities:

The notion of granting AI systems some form of legal personhood or agency, a topic of ongoing debate, introduces another layer of complexity to the discussion of liability. This would necessitate rethinking legal frameworks to accommodate non-human actors within the legal system.

Paragraph 2: Legal and Ethical Frameworks - A Deeper Dive

The development and implementation of legal and ethical frameworks to govern AI use and prevent AI crimes require global collaboration and foresight. This includes not only the creation of laws and regulations but also the establishment of international norms and agreements to ensure consistent standards across borders. Furthermore, these frameworks must be dynamic, capable of evolving alongside AI technologies to address new challenges as they arise.

1. Case Studies and Precedents:

Examining case studies of AI crimes and the responses of different jurisdictions can provide valuable insights into effective strategies for combating these issues. Legal precedents, where courts have addressed AI-related offenses,

offer a foundation upon which to build and refine legal doctrines pertaining to AI crimes.

2. Public Awareness and Education:

Elevating public understanding of AI crimes and the legal mechanisms in place to address them is essential for prevention and deterrence. Educational initiatives aimed at both the general public and specific industries can empower individuals and organizations to recognize, report, and mitigate the risks associated with AI technologies. (United Nations Interregional Crime and Justice Research Institute [UNICRI], 2021)

SECTION 2: LEGAL FRAMEWORK AND SANCTIONS FOR AI CRIMES

Subsection 1: Comparative Analysis of AI Crime Legislation

The legal landscape for AI crimes is as varied as the technology itself, with different jurisdictions taking unique approaches to regulation and enforcement. A comparative analysis reveals a spectrum of legislative frameworks, from highly detailed to more general, reflecting the diverse legal, cultural, and technological environments across the globe.

1. Algeria:

As a representative of a non-Western jurisdiction, Algeria's approach to AI crime is largely based on its general cybercrime laws, outlined in the Penal Code and specific regulations addressing digital crimes. The country has yet to adopt AI-specific legislation, relying instead on broader legal principles to tackle AI-related offenses. (Algerian Penal Code, 2021)

2. United States:

The U.S. has approached the regulation of AI through a combination of sector-specific laws and broader legislative frameworks that address data protection, privacy, and cybersecurity. While there is no comprehensive AI-specific criminal law, existing legislation such as the Computer Fraud and Abuse Act (CFAA) has been applied to AI-related offenses. (United States Department of Justice, n.d.)

3. European Union:

The EU has been proactive in establishing regulations that indirectly affect AI, notably through the General Data Protection Regulation (GDPR), which includes provisions relevant to AI, such as the right to explanation. Moreover, the EU has proposed the Artificial Intelligence Act, aiming to create a harmonized regulatory framework for AI across member states, focusing on safety, transparency, and accountability. (United Nations, 2020)

4. China:

China's approach to AI regulation emphasizes state control and technological advancement, with specific plans for AI development and ethics guidelines. While

comprehensive AI-specific criminal laws are not yet in place, existing cybersecurity and data protection laws have been used to govern AI technologies. (Cyberspace Administration of China, 2017)

These examples illustrate the range of regulatory strategies, from preemptive and detailed legislation in the EU to more reactive and general approaches in countries like Algeria. The effectiveness of these legal frameworks in addressing AI crimes is an ongoing subject of debate among scholars and policymakers.

Subsection 2: The Role of International Cooperation and Ethics in AI Crime Regulation

The global proliferation of artificial intelligence (AI) technologies and the transnational nature of AI crimes underscore the critical need for robust international cooperation and the integration of ethical considerations into regulatory frameworks. Effective responses to AI-related criminal activities necessitate collaboration among nations, international organizations, and stakeholders across various sectors.

Paragraph 1: Enhancing International Cooperation:

1. Multilateral Organizations:

Entities such as the United Nations (UN), the International Criminal Police Organization (Interpol), and the European Union Agency for Cybersecurity (ENISA) serve as focal points for international cooperation on AI crime regulation. These organizations facilitate information exchange, coordinate joint investigations, and provide technical assistance to member states. (Montreal Declaration for a Responsible Development of Artificial Intelligence, 2018)

2. Bilateral Agreements:

Bilateral agreements between countries can enhance cooperation in combating AI crimes, enabling the sharing of intelligence, resources, and expertise. These agreements can foster closer collaboration in areas such as data sharing, extradition, and joint law enforcement operations.

3. Public-Private Partnerships:

Collaboration between governments, law enforcement agencies, and private sector entities is essential for addressing AI crimes effectively. Public-private partnerships can leverage industry expertise, technological capabilities, and resources to develop innovative solutions and strengthen cybersecurity measures. (Beijing AI Principles, 2019)

Paragraph 2: Ethical Considerations and Guiding Principles:

1. Transparency and Accountability:

Ethical frameworks for AI should prioritize transparency and accountability in AI development, deployment, and use. This includes ensuring transparency in AI algorithms and decision-making processes, as well as accountability mechanisms for AI-driven actions.

2. Non-Discrimination and Fairness:

Ethical guidelines must address concerns related to bias, discrimination, and fairness in AI systems. Efforts should be made to mitigate biases in data collection, algorithm design, and decision-making processes to ensure equitable outcomes for all individuals and communities.

3. Respect for Human Rights:

AI technologies should be developed and deployed in a manner consistent with international human rights standards. This includes respecting privacy rights, freedom of expression, and the right to due process, among others.

4. Societal Impact Assessment:

Ethical considerations should extend to the broader societal impact of AI technologies, including their implications for employment, inequality, and social cohesion. Societal impact assessments can help identify and address potential risks and harms associated with AI deployment.

Paragraph 3: Integration of Ethical Considerations into Legal Frameworks:

1. Legislative Alignment:

Legal frameworks should align with ethical principles and guidelines for AI governance, ensuring that regulatory responses to AI crimes are grounded in ethical norms and values.

2. Ethics by Design:

The concept of ethics by design advocates for integrating ethical considerations into the design and development of AI systems from the outset. By embedding ethical principles into AI technologies, developers can proactively address potential risks and mitigate ethical dilemmas. (Scherer, 2016, p. 25)

3. Oversight and Enforcement:

Regulatory agencies should have mechanisms in place to monitor compliance with ethical standards and enforce legal obligations related to AI governance. This may include conducting audits, investigations, and imposing sanctions for violations of ethical guidelines. (Casey et al., 2019, p.65)

International cooperation and ethical considerations are indispensable pillars of effective AI crime regulation. By fostering collaboration among nations, promoting ethical best practices, and aligning legal frameworks with societal values, stakeholders can work together to address the multifaceted challenges posed by AI technologies while upholding fundamental rights and principles. This integrated approach is essential for building trust in AI systems and ensuring their responsible and ethical use in a rapidly evolving digital landscape.

SECTION 3: CHALLENGES AND PERSPECTIVES IN ADDRESSING AI-RELATED CRIMINAL ACTIVITIES

Subsection 1: Technological Evolution and Legal Adaptation

The rapid pace of technological advancements in artificial intelligence (AI) presents significant challenges to existing legal frameworks worldwide. These frameworks, often developed in an era predating the current technological landscape, struggle to accommodate the novel and complex issues raised by AI. This misalignment necessitates ongoing adaptation to ensure laws remain effective and relevant.

Paragraph 1: Technological Evolution

The rapid evolution of artificial intelligence (AI) technologies has ushered in a new era of innovation and complexity, presenting unprecedented challenges to existing legal frameworks. AI technologies are advancing at an exponential rate, outpacing the traditional legislative processes designed to regulate them. This phenomenon often results in a significant lag in legal responses to emerging challenges posed by AI-driven systems (Scherer, 2016, p.25).

For instance, the development of autonomous vehicles has raised intricate legal questions regarding liability in the event of accidents or malfunctions. Similarly, the integration of AI into medical diagnostics introduces complex ethical and legal considerations surrounding patient consent, data privacy, and medical malpractice (Casey et al., 2019, p.66).

Additionally, the use of AI algorithms in financial trading has transformed market dynamics, necessitating novel regulatory approaches to ensure market stability and investor protection (European Commission, 2021).

These examples underscore the pressing need for lawmakers and legal scholars to adapt existing legal frameworks to the rapid pace of technological innovation in the AI domain.

Paragraph 2: Legal Adaptation:

Adapting legal frameworks to keep pace with AI involves several key challenges:

1. Understanding AI:

Legal systems must develop a deep understanding of AI technologies and their potential uses and abuses. This requires interdisciplinary collaboration between technologists, legal experts, and policymakers. (Floridi & Cowls, 2019, p. 123)

2.Flexibility:

Laws must be flexible enough to address the rapid evolution of AI while ensuring stability and predictability for those subject to the laws.

3.Global Consistency:

AI operates on a global scale, necessitating legal frameworks that are consistent across jurisdictions to prevent regulatory arbitrage. (Veale & Edwards, 2018, p. 101)

Examples of adaptation include the European Union's General Data Protection Regulation (GDPR), which introduces concepts of data protection by design and by default, and the discussions around the ethical guidelines for AI development and use.

Subsection 2: Balancing Innovation and Regulation

Striking a balance between fostering innovation in AI and ensuring its ethical use and regulation is a critical challenge for policymakers and stakeholders. On one hand, over-regulation could stifle technological advancement and limit the potential benefits of AI. On the other, insufficient regulation could lead to abuses and harm to individuals and society. (European Commission, 2020, p. 456)

Paragraph 1: Innovation

Encouraging innovation in AI requires a supportive ecosystem that includes funding for research, education to develop skilled professionals, and legal frameworks that enable experimentation and development. (Veale & Edwards, 2018, p. 101)

Paragraph 2: Regulation

Effective regulation should protect against harms without unduly limiting the potential of AI. This includes mechanisms for accountability, transparency in AI decision-making processes, and protections against misuse.

Paragraph 3: Strategies for Balance**1. Regulatory Sandboxes:**

Creating environments where new AI technologies can be tested under regulatory supervision allows for innovation while ensuring oversight.

2. Ethical AI Frameworks:

Developing and implementing ethical guidelines for AI research and development can guide innovators while safeguarding societal values. (Wachter et al., 2017, p. 789)

3. Stakeholder Engagement:

Involving a broad range of stakeholders in the development of AI regulations ensures diverse perspectives are considered, balancing the needs of innovators with those of society at large.

Conclusion

The exploration of criminal liability arising from the use of artificial intelligence (AI) illuminates the multifaceted challenges and opportunities presented by this technological evolution. This study has traversed the landscape of AI crimes, the intricate web of responsibilities among creators, users, and regulators, and the existing legal frameworks that aim to address these issues.

It has also delved into the dynamic interplay between rapid technological advancements and the legal adaptation required to manage them effectively, alongside strategies to balance innovation with ethical considerations and regulation.

The main findings underscore the complexity of attributing criminal liability in the context of AI, given the autonomous and opaque nature of these technologies. AI crimes, characterized by their technical sophistication and the difficulty in establishing intent, present unique challenges to traditional legal frameworks. The roles of creators, users, and regulatory bodies are crucial in navigating these challenges, each bearing different degrees of responsibility and capacity for oversight.

Comparative analysis across jurisdictions revealed a fragmented landscape of laws and regulations, highlighting the need for coherent legal standards and international cooperation. Furthermore, the rapid pace of AI development necessitates continuous legal adaptation, underscoring the importance of flexibility, global consistency, and interdisciplinary collaboration in legal responses.

For policymakers, the findings emphasize the urgency of developing legal frameworks that can keep pace with technological advancements, ensuring that laws are both effective and adaptable. Legal practitioners are called to deepen their understanding of AI technologies and their societal implications, equipping them to navigate the emerging legal landscape. Technologists, on the other hand, are encouraged to engage with ethical considerations and regulatory standards from the outset of AI development, fostering responsible innovation.

Recommendations

1. **Legal Reforms:** To address the gaps and inconsistencies identified, comprehensive legal reforms are essential. These reforms should aim to clarify liability in AI contexts, update definitions of criminal conduct to encompass AI-specific activities, and establish guidelines for the ethical use of AI technologies.
2. **International Collaboration:** Enhancing international cooperation is critical for combating AI crimes effectively. This entails developing common legal standards, facilitating cross-border law enforcement efforts, and sharing best practices for regulating AI technologies.

3. **Ethical Guidelines:** Integrating ethical considerations into the development and regulation of AI is paramount. This involves creating and adhering to ethical guidelines that prioritize human rights, transparency, and accountability, ensuring AI technologies serve the public good while mitigating risks of misuse.

The journey through the legal and ethical landscape of AI criminal liability reveals a complex but navigable terrain. By embracing continuous adaptation, fostering international collaboration, and integrating ethical considerations, society can harness the benefits of AI while safeguarding against its potential harms. This balanced approach is crucial for ensuring that the development and use of AI technologies reflect the values and norms of a just and equitable society.

References

- Algerian Penal Code. (2021.). Articles related to cybercrime and digital security. Retrieved from [https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria]
- Beijing AI Principles. (2019). Principles for the Governance of AI. Retrieved from [https://ai-ethics-and-governance.institute/team/]
- Casey, B., Farhangi, A., & Vogl, R. (2019). Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. *Berkeley Technology Law Journal*, 34(1).
- CMS Legal. (2021, March 5). Data protection and cybersecurity laws in Algeria. CMS Expert Guide. Retrieved from https://cms.law
- Cyberspace Administration of China. (2017). China's New Generation of Artificial Intelligence Development Plan. Retrieved from [https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/]
- European Commission. (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust.
- European Commission. (2021). Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Retrieved from [https://merlin.obs.coe.int/article/9203]
- Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*.
- Montreal Declaration for a Responsible Development of Artificial Intelligence. (2018). Retrieved from [https://monoskop.org/images/d/d2/Montreal_Declaration_for_a_Responsible_Development_of_Artificial_Intelligence_2018.pdf]
- Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2).
- United Nations Interregional Crime and Justice Research Institute (UNICRI). (2021). Artificial Intelligence and Robotics for Law Enforcement.
- United Nations. (2020). Activities of the United Nations in Combating Cybercrime. Retrieved from [https://www.unodc.org/unodc/en/cybercrime/home.html]
- United States Department of Justice. (n.d.). Computer Fraud and Abuse Act (CFAA). Retrieved from [https://www.justice.gov/jm/jm-9-48000-computer-fraud]
- Veale, M., & Edwards, L. (2018). Clarity, Surprises, and Further Questions in the Article 22 GDPR Guidance. *European Data Protection Law Review*.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*.