Ethics in using AI in law enforcement operations

Adrian Luca
AI Multimedia Lab
National University of Science and Technology POLITEHNICA Bucharest
Bucharest, Romania
adrian.luca2904@stud.etti.upb.ro

Bogdan Ionescu
AI Multimedia Lab
National University of Science and Technology POLITEHNICA Bucharest
Bucharest, Romania
bogdan.ionescu@upb.ro

***Abstract*—This paper is about ethics in using AI in law enforcement at operational level. I have tried to identify ethical problems that could occur from using AI algorithms in law enforcement operational field. This ethical issues refers not only to using big data but also in biases that could be encountered while running this kind of operative algorithms, the biggest problems arising from how the data is being used.**

***Index Terms*—ethic, AI, law enforcement, human rights, bias, data, transparency**

I. Introduction

In an era when ubiquitously generated and extensively utilized data drives decision-making and innovation, ensuring the compliance, fairness, and environmental sustainability of ML/AI operations has become paramount. The disruptive emergence of new AI models, the increasing volume of data, the complexity and computational needs of AI systems, the interaction of different and often competing actors and the multitude of emerging legislations pose significant compliance challenges with regulations such as the General Data Protection Regulation, the Data Governance Act, the Data Act, and the Artificial Intelligence Act. Moreover, there is an increasing societal and business demand for ethical and transparent AI and an urgent need to mitigate the environmental impact of data and AI operations aligning with the European Green Deal's objectives.

II. Research idea

In my research paper, I want to emphasize the challenges that could occur to law enforcement agencies (LEAs) while integrating different artificial intelligence architectures to work with big data collection in their process to analyze information to solve or prevent complex criminal activities like organized crime networks, terrorism, human trafficking, fraud and financial crimes, cybercrime, and other clandestine activities that pose significant threats to the safety and security of communities. Traditional methods used by intelligence analysts often fall short in addressing these challenges, necessitating the adoption of advanced AI techniques to enhance decision-making and operational efficiency while showing compliance with ethics and data protection regulations. Traditionally, AI developments neglect inherent mechanisms to ensure compliance with various legislation and ethical guidelines and commonly treat compliance as an afterthought and AI explainability principle about the functioning of AI and its outcomes needs to be provided [1]. This oversight presents a significant challenge as the demand for compliance in data operations grows alongside data and AI systems' increasing complexity and scale. Integrating compliance, fairness and environmental sustainability into AI operations is more critical than ever, especially considering the European Green Deal's ambitious goals and European Convention of Human Rights who are calling for caution in the development and usage of AI within the European Union [2]. Addressing the gap between existing AI architectures and the requirements for legal, ethical, and environmental compliance remains uncertain in different aspects, underscoring the urgency and relevance of clear and stated regulations for the organizations.

III. Moral and ethical alignment

Can AI algorithms align with human values? While being deployed, an AI system should reflect ethical principles aligned with our values while running different services in order to help us. This requires ongoing effort to define and program moral framework into AI, particularly in areas with subjective or complex ethical considerations, such as social justice. While implementing moral frameworks into AI systems, different elements should be taken into consideration: [3]

A. Privacy concerns

AI systems rely on vast amounts of data to properly work, which includes personal information collected from users or persons who get in contact in different ways with the systems. This raises serious privacy issues because users may be unaware of how much data is collected, how it's stored, and who has access to it. For example, facial recognition or profiling technology used in public spaces could lead to constant surveillance, potentially creating the premises for a society where individuals are constantly tracked without their consent. Privacy concerns in AI also extend to data security, as systems could be hacked or third-party companies as technology providers could have access to sensitive information, impacting user trust and potentially causing harm to persons. [4]

1st Workshop on Artificial Intelligence for Multimedia, AI Multimedia Lab, CAMPUS Research Institute, POLITEHNICA Bucharest, Bucharest, Romania, 8 November, 2024

B. Informed consent

To have a moral and ethical approach of using AI systems user should be aware that their data is being collected and it could probably influence their decision. Informed consent ensures users are aware of the implications of AI on their personal data, how it will be used, and what potential risks may exist. [5]

C. Bias in AI systems

AI systems rely on algorithms that can analyze patterns in large datasets, but these algorithms can also lead to biased outcomes. Data usage might reinforce existing stereotypes or prejudices, particularly against marginalized groups. For example, predictive policing algorithms, which rely on historical crime data, might unfairly target certain communities, leading to over-policing of minority populations. Such practices raise concerns about discriminatory data usage. [6]

D. Fairness and Due Process

AI systems used in decision-making processes—such as in criminal justice, financial, or social services—must adhere to principles of fairness and provide individuals with due process. Fairness ensures that AI does not arbitrarily or disproportionately impact certain groups, while due process allows individuals affected by AI decisions to contest or appeal these outcomes. Ensuring fairness in AI requires transparent criteria and oversight to protect individuals' rights, particularly when automated decisions could have lasting consequences on their lives.

E. Transparency

Transparency in AI refers to the openness about how AI systems work, the data they use, and the decision-making criteria they apply. Without transparency, it is difficult for users, regulators, or other stakeholders to understand, evaluate, or trust AI systems. Transparent AI practices are essential for accountability, enabling external parties to audit the technology for fairness, accuracy, and compliance with ethical standards.

F. Accountability

As AI becomes more autonomous, the line between human and machine responsibility can blur. Clear accountability structures are needed, particularly in critical areas like justice, profiling, crime prevention. Without clear accountability, it's challenging to assign responsibility, especially in cases of unintended harm or biased outcomes.

G. Overreliance on Technology

As AI becomes more integrated into society, there is a risk of overreliance on technology, potentially diminishing human oversight and critical thinking. Overreliance on AI can lead to automation bias, where users may trust AI decisions even when they are incorrect or flawed. This can be particularly dangerous in sectors like law enforcement, where a human element is crucial for ethical considerations. Balancing AI-driven efficiency with human judgment is vital to prevent dependence on technology and ensure decisions remain nuanced and contextually appropriate.

H. Security and Risk Management

AI systems can be targets for cyber attacks, where inputs are subtly manipulated to produce harmful or wrong outputs. Ensuring robust security practices in AI development and deployment is crucial for preventing malicious misuse, especially in areas like national security and critical infrastructure.

CONCLUSION

The integration of AI in law enforcement presents significant opportunities to enhance decision-making and operational efficiency in working and combating complex crimes. However, this potential comes with serious ethical responsibilities, especially regarding data privacy, informed consent, bias, fairness, transparency and accountability. As AI systems become increasingly autonomous and embedded in high-stakes areas like criminal justice, the risk of unintended harm and rights violations rises, making it essential to adopt ethical safeguards and regulatory compliance from the outset.

Ensuring that AI aligns with human rights values and adheres to principles of fairness and due process is not only a technical challenge but also a moral imperative. To responsibly leverage AI's benefits while mitigating risks, law enforcement agencies must implement robust policies that enforce ethical standards, enable transparency, and ensure accountability. As regulations like the GDPR and the Artificial Intelligence Act continue to shape the landscape, the need for ethical, fair and environmentally sustainable AI practices will only grow.

Ultimately, the path forward requires a collaborative approach among developers, policymakers, and law enforcement agencies to build AI systems that are not only effective but also equitable and respectful of human rights. Addressing these ethical challenges head-on will enable AI to serve as a tool for societal good, while protecting the dignity, privacy and security of all individuals.

REFERENCES

[1] R. Matulionyte, A. Hanif, "A call for more explainable AI in law enforcement." pp. 75-80. 10.1109/EDOCW52865.2021.00035, 2021.
[2] S. Roksandić, N. Protrka and M. Engelhart, "Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?," 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO),pp. 1225-1232, Opatija, Croatia, 2022.
[3] G. Iason. (2020). Artificial Intelligence, Values, and Alignment. Minds and Machines. 30. 411-437. 10.1007/s11023-020-09539-2.
[4] Devineni, S. Karthik. (2024). AI in Data Privacy and Security.. International Journal of Artificial Intelligence and Machine Learning. 3. 35-49.
[5] M. Jones, E. Kaufman, E. Edenberg, "AI and the Ethics of Automating Consent. IEEE Security and Privacy" pp. 64-72. 10.1109/MSP.2018.2701155, 2018.
[6] T. Sorell, "AI-related data ethics oversight in UK policing", "Policing: A Journal of Policy and Practice" pp. 16, 2024.