Europol Report: Benefits and Challenges of AI for Law Enforcement

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Cornelia Riehle

AUTHOR
Cornelia Riehle
Deputy Head of Section
Academy of European Law

Published in
2024, Vol. 19(3) eucrim
ISSN: 1862-6947
https://eucrim.eu

For the first time, Europol's Innovation Lab has published an Observatory Report on AI and Policing, which aims to provide an overview of the benefits and challenges associated with the adoption of artificial intelligence (AI) by law enforcement. The report seeks to show how the rapidly evolving AI technology can contribute to enhancing the efficiency, effectiveness, and overall performance of law enforcement operations, while upholding ethical and legal standards. It is primarily aimed at Law Enforcement Agencies (LEA) operating across the EU but should also be of value to other readers, such as policymakers, technology developers, academics, civil rights advocates, and the general public, both within the EU and globally.

The report looks at applications of AI in law enforcement, such as data analytics, digital forensics, computer vision, and biometrics, and generative AI. It goes on to analyse technological limitations and challenges as well as ethical and social issues in AI for law enforcement, for example data bias and fairness, privacy and surveillance, accountability and transparency, and human rights and discrimination. It also provides an overview of the objectives, scope, and key provisions of the EU Artificial Intelligence Act and its implications for law enforcement agencies. The report concludes with an outlook and a set of key takeaways, including:

- The potential of AI to significantly transform policing – from advanced criminal analytics that reveal trends in vast amounts of data, to biometrics that allow the prompt and unique identification of criminals;
- The ability to integrate large and complex datasets and natural language processing into policing applications allows for the extraction of actionable insights, and improves resource forecasting and operational efficiency, while these technologies can simultaneously protect and uphold privacy rights;
- AI-driven tools, including in the context of OSINT and SOCMINT, that can process unstructured data to provide real-time insights are improving the ability of law enforcement to more effectively and efficiently address urgent situations such as crimes against children and terrorism;
- Technologies like machine translation are crucial to facilitate international collaboration among law enforcement agencies;
- The fusion of AI and biometrics can enhance criminal identification accuracy while protecting the privacy of non-relevant individuals;
- Generative AI represents the next leap, from passive analysis to active creation, and offers many opportunities for law enforcement. But as with any tool, its power lies in its judicious and ethical use, balancing innovation with responsibility;

- Substantial technological infrastructure and expertise is required to effectively develop and deploy AI technologies, which presents significant challenges, particularly for smaller law enforcement agencies;
- To ensure appropriate data handling and responsible data processing practices, law enforcement agencies must invest in training and raising awareness amongst their staff to navigate these complex legal and ethical landscapes;
- Compliance with the EU AI Act represents a crucial balancing act, as it requires law enforcement to adhere to stringent ethical, legal, and privacy standards, potentially necessitating the reassessment of existing AI tools;
- The EU AI Act challenges law enforcement agencies to allocate additional resources and navigate the complexities of compliance. This is especially relevant for those agencies developing AI tools in house, emphasising the need for a responsible and ethical approach to AI integration in law enforcement;
- Police forces, which may already be utilising certain AI systems, will face the challenging task of re-evaluating these tools. Should any of these operational technologies fall within the prohibited category set by the EU AI Act, they would need to be deactivated, leading to potential challenges in maintaining operational continuity;
- Addressing bias in AI is paramount, with a need for systems that are not only technically sound but also embody fairness, justice, and impartiality, ensuring that data collection and storage adhere to strict privacy guidelines;
- Accountability, transparency, and explainability are essential, not only for ethical and responsible AI use but also to ensure that evidence collected and analysed by AI systems withstands scrutiny, respect the right to a fair trial, and is deemed acceptable in court proceedings;
- Regular audits of AI systems are essential to ensuring compliance with established privacy and data protection standards, maintaining a balance between harnessing AI-driven insights and safeguarding fundamental rights and individual freedoms.

Looking to the future, quantum computing, 6G connectivity, automated drones and robotics, AI chips, and edge computing are on the verge of opening up new possibilities for law enforcement, if used ethically and in accordance with the principles of justice and fairness. Public trust and acceptance are seen as cornerstones for the successful integration of AI technologies into law enforcement. The report therefore emphasises the need to invest in community engagement, education, and feedback mechanisms. Lastly, strengthening collaboration and knowledge sharing in the form of inter-agency cooperation, partnerships with academia and industry, and engagement with civil society, among others, is seen as essential to the success of integrating AI into law enforcement.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union