The limits of Government Surveillance: Law enforcement in the Age of Artificial Intelligence

Panagiotis Kitsos, PhD.
Hellenic Open University,
Institute for Internet & the Just Society
Athens, Greece

ABSTRACT

Artificial intelligence applications used by law enforcement agencies are the principal element of investigation in this paper. A brief presentation and description of the various tools based on artificial intelligence, depending on their scope, is attempted, while at the same time the obvious and not that obvious implications of the adoption of such methods are discussed, namely the setbacks created by the so-called algorithmic bias, the risks on fundamental human rights involved in mass surveillance and privacy and data protection issues that arise from the handling of AI applications by individuals active in law enforcement. The article also discusses the potential solution to such concerns, which would be the adoption of a set of rules and measures on ethical and legal governance ,and at the same time, it attempts to offer some guidance on the implementation of regulatory provisions that would help establish a sense of trust and security for individuals that would otherwise question the expediency of the wider use of AI applications by government bodies involved in law enforcement.

Keywords

Artificial intelligence, law enforcement, data protection, privacy

1. INTRODUCTION

Artificial Intelligence is becoming a term that apart from encompassing an ever-growing number of Information and Communication Technology applications is changing the world through the transformation of various aspects of human activity, from business and economy to health care and law enforcement. As it evolves, "it magnifies the ability to use personal information in ways that can intrude on privacy interests by "raising the analysis of personal information to new levels of power and speed"[1] triggering an intense debate among Academia, Government, Tech Companies and NGOs on how to efficiently address these issues. In order to control and regulate the growing ecosystem of artificial intelligence methods and applications a number of soft [2]and hard law[3] initiatives have been adopted at international level.[4][5]

It seems though that there are a number of artificial intelligence threats for human rights coming directly from the use of these technologies by the state. Governments are faced with a growing demand to secure public safety and security and law enforcement agencies are dealing with a variety of traditional crime such as homicide, theft, white collar crime etc or new ones such as cyber-related and cyber dependent crimes. Add to these challenges the ever increasing transnational nature of crime and it becomes more than evident that law enforcement, in order to prevent and reduce crime, requires new advanced structures with efficient allocation of operational capabilities, skilled staff, effective efficient and "intelligent" instruments and methods to combat its adversaries.

This presentation is designed not as a comprehensive list of the issues surrounding the use of artificial intelligence by police force. Instead is a starting point of research on issues related to the ongoing developments on the matter.

To achieve that objective, we will present an overview of the artificial intelligence applications used by law enforcement agencies and describe the issues arising from the use these new technologies by the law enforcement. Lastly we examine the ethical and regulatory framework that governments and law

[1] Cameron F. Kerry. (2020, February 10). Protecting privacy in an AI-driven world. Retrieved from:https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

[2] the term "soft law" is used to denote non legally binding documents, either agreements, principles or declarations that serve as guidelines. The term is frequently used in the international sphere. OECD resolutions and Codes of Conduct are examples of such non binding documents

[3] the term «hard law refers to legally binding obligations deriving from either legal isntruments or binding agreements that can be enforced before a competent court. An example of such a binding legal instrument is the General Data Protection Regulation

[4] In 2019 the framework of OECD the first international accord on AI development was adopted with the aim to ensure that AI systems are robust, safe, fair and trustworthy See OECD (2019, May 22) Forty-two countries adopt new OECD Principles on Artificial Intelligence. Retrieved from: https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm In February 2020 the European Commission published a White Paper on Artificial Intelligence. See European Commission (2020, February 19). White Paper on Artificial Intelligence: a European approach to excellence and trust. Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf and European Commission. High-Level Expert Group on AI (2019, April 8). Ethics Guidelines for Trustworthy Artificial Intelligence. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[5] European Commission (2020, February 19). White Paper on Artificial Intelligence: a European approach to excellence and trust. Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

WAIEL2020, September 3, 2020, Athens, Greece

enforcement agents need to follow in order to safeguard citizens rights.

2. ARTIFICIAL INTELLIGENCE AND LAW ENFORCEMENT

Security and public safety are key prerequisites in the function of societies. Citizens expect governments to fight crime and disorder as a means to preserve a safe environment where private life is protected and respected and business is allowed to flourish. These rather common observations bare a significant weight in modern era where traditional crime is evolving enabled by the exponential growth of the technology which creates an evolving, extremely complex, rapidly shifting, and increasing technology-enabled, globalised crime and terrorism landscape. A complex ecosystem of traditional, cyber-dependent[6] and cyber-enabled[7] crimes that is challenging and altering police work.[8]

To meet these challenges, law enforcement as an information based activity [9] encompasses new technologies that process these volumes of data in order to identify and prevent crime. The amount of data generated by the use of information and communication technologies creates huge potential for the Big Data analytics and artificial antelligence technologies and automated decision systems that now are able to extract and analyze data more efficiently and at a rapid pace. [10]

Artificial intelligence is used in many fields like advertising, finance, marketing, healthcare, transportation, media , e-commerce, energy but they are also used by law enforcement agencies.

Law enforcement agencies are increasingly aware of the potential of artificial intelligence in the fight against crime; Artificial intelligence technologies have long been adopted for the facilitation of crime investigation, namely platforms that enable the collection and analysis of evidence material[11]. In addition to that, law enforcement agencies have also opted for the use of tools that can enable the police to make snap decisions in particularly high-risk situations i.e. when human lives are threatened. These situations may vary from victim rescue to the apprehension of possible suspects. In the light of the covid-19 pandemic, AI is continuously being invoked in order to help control the spread and predict the path that the virus might take within specific zones. Thus, the allocation of forces to where they are mostly needed is optimized.[12]

Law enforcement agencies have adopted a variety artificial intelligence related applications: [13]

1. Visual processing is the interpretation and understanding of visual information that allows us to identify what we see, to interpret size, shape, distances etc. From a technological perspective, visual processing, or computer vision, is the mimicry of the human visual system by a machine and it concerns the extraction, analysis and understanding of information from images.
    a. facial recognition technologies,
    b. automated number plate recognition
    c. lip-reading technologies,
    d. Surveillance Drones
    e. body-worn cameras (bodycams)
    f. closed-circuit television (CCTV)
2. Audio processing with speaker and speech identification,
3. Aural surveillance (i.e. gunshot detection algorithms),
4. Autonomous research and analysis of identified databases,
5. Forecasting (predictive policing and crime hotspot analytics),
6. Behaviour detection tools, autonomous tools to identify financial fraud and terrorist financing, social media monitoring (scraping and data harvesting for mining connections),
7. Social media monitoring
8. International mobile subscriber identity (IMSI) catchers,
9. Automated surveillance systems incorporating different detection capabilities (such as heartbeat detection and thermal cameras);

[6] According to (IOCTA) Report , cyber-dependent crime can be defined as any crime that can only be commited using computers, computer networks or any other forms information communication technology see EUROPOL.(2019) Internet Organised Crime Threat Assessment (IOCTA) Report . Retrieved from https://www.europol.europa.eu/iocta-report

[7] According to Interpol.'Traditional' crimes which are facilitated by technology. For example, theft, fraud, even terrorism. Interpol, Cybercrime.Retrieved from file:///C:/Users/user/Downloads/Cybercrime.pdf

[8] Deloitte Insights (2019, October 20) The future of law enforcement. Policing strategies to meet the challenges of evolving technology and a changing world. Retrieved from https://www2.deloitte.com/us/en/insights/focus/defense-national-security/future-of-law-enforcement-ecosystem-of-policing.html

[9] McCarthy, O. J. (2019). *AI & Global Governance: Turning the Tide on Crime with Predictive Policing - United Nations University Centre for Policy Research.* United Nations University Centre for Policy Research. Retrieved from https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html

[10] Artifcial intelligence (AI): the field of computer science dedicated to solving cognitive problems commonly associated with human intelligence. An example of AI in policing is the algorithmic process that supports facial recognition technology.

[11] Such tools would inlcude ADS (automated decision systems): computer systems that either inform or make a decision on a course of action to pursue about an individual or business that may or may not involve AI. (Grimond W., Singh A. ,A Force for Good?, RSA 2020, retrieved at https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf). An example of ADS in policing would be where facial recognition technology alerts to wanted suspects in a crowd.

[12] Smith, L. (2020, June 3) The Long (and Artificial) Arm of the Law: How AI is Used in Law Enforcement.Datanami. Retrieved from https://www.datanami.com/2020/06/03/the-long-and-artificial-arm-of-the-law-how-ai-is-used-in-law-enforcement/

[13] Some AI related applications are described in a draft report issued by the European Parliament LIBE Committee on Civil Liberties, Justice and Home Affairs. See LIBE Committee on Civil Liberties, Justice and Home Affairs (2020) Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters. Available at https://www.europarl.europa.eu/committees/el/libe/documents/latest-documents

10. Biometric identification

11. Natural Language Processing (NLP) – otherwise known as computational linguistics – is a field of AI that, in essence, enables machines to read, understand and derive meaning from human languages. It has proven useful in the extraction of information from large datasets, especially those containing unstructured data – data that is not or cannot be contained in a row-column format - like the text of an email. In light of this, NLP has found its way in daily life, such as in many applications that provide predictive or suggestive text and word or grammar checks.

3. IMPLICATIONS

Law enforcement agencies across the globe have embraced new technologies but already a number of human rights implications are obvious by the systematic use of these technologies.

The most obvious implications are the discriminatory profiling created by the algorithmic biases,[14] the loss of anonymity from the creation of a mass government surveillance and the erosion of privacy.

3.1 Algorithmic bias [15]

The use of artificial intelligence by law enforcement agencies to analyze vast data sets produced by a variety of todays ICTs in order to either evaluate whether someone (individuals or groups) is likely to commit a crime in the future the so called "predictive-policing" raises important ethical and legal concerns.[16]

A study from the Royal United Services Institute (RUSI) in 2019 warned that "Algorithms that are trained on police data 'may replicate (and in some cases amplify) the existing biases inherent in the dataset', such as over or under-policing of certain communities, or data that reflects flawed or illegal practices." According to the study a police officer commented that 'young black men are more likely to be stop and searched than young white men, and that's purely down to human bias. That human bias is then introduced into the datasets, and bias is then generated in the outcomes of the application of those datasets'. It is obvious that people from disadvantaged backgrounds are label as as "a greater risk" since they were more likely to have contact with public services, thus generating more data that in turn could be used to train the AI.[17] The adverse effects of these procedures have been revealed in a number of cases where police «smart»technology to predict and prevent crime

In a 2018 article in The Verge was revealed that the City of Orlando in 2012 entered to a secret agreement with the data-mining firm Palantir to deploy a predictive policing system.[18] The system used biased historical data such as arrest records and electronic police reports, to forecast crime.[19] The case triggered a nation wide discussion on effectiveness of predictive policing the advesrse effects on privacy and the need for transparency.[20]

Just a few days ago in New York an African American man, was arrested after a detroit police facial recognition system wrongfully matched his photo with security footage of a shoplifter. According to New York Times the man was arrested and handcuffed in front of his wife and two young daughters.[21] The American Civil Liberties Union (ACLU) has already filed a formal complaint against Detroit police over what it says is the first known example of a wrongful arrest caused by faulty facial recognition technology.

The methods of predictive policing and especially the use of facial recognition has triggered a widespread reactions from journalists, scholars, civil liberties organizations.

On june 10th Amazon announce a one-year moratorium on police use of its facial-recognition technology, yielding to pressure from police-reform advocates and civil rights groups.[22]

3.2 Mass Surveillance

Police surveillance has always been of instrumental importance for governments. In the aftermath of Snowden's revelations that U.S and European law enforcement agencies and secret services are actually conducting mass scale surveillance of their citizens' electronic communications a wider discussion has been launched on the necessity and methods of police surveillance.[23]

The combined use of a variety of Internet and digital technologies with methods that use artificial intelligence creates a complex surveillance ecosystem that monitors people's lives and results in a loss of anonymity of unprecedented scale.

[14] Mann, M., Matzner T. , Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (July 2019) Big Data and Society, vol 6, iss. 2 (2019), retrieved from https://journals.sagepub.com/doi/10.1177/2053951719895805#

[15] According to oxford dictionary "bias" is an inclination or prejudice for or against a person or group, especially in a way that is considered to be unfair." Retrieved from https://www.lexico.com/definition/bias

[16] Richardson R. et all. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems and Justice (February 13, 2019) 94 N.Y.U L.Rev.online 192 (2019). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423

[17] Babuta, A., Oswald, M. (2019) Data Analytics and Algorithmic Bias in Policing, RUSI Briefing Paper. Available at https://rusi.org/sites/default/files/20190916_data_analytics_and_algorithmic_bias_in_policing_web.pdf

[18] The agreement had never passed through a public procurement process.

[19] Hao, K. (2019, February 19). Police across the US are training crime-predicting AIs on falsified data. MIT Technology Review. Retrived from https://www.technologyreview.com/2019/02/13/137444/predictive-policing-algorithms-ai-crime-dirty-data/

[20] Winston A. (2018, February 27). Palantir has secretly been using New Orleans to test its predictive policing technology. The Verge. Retrieved from https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

[21] Kasmiir Hill (2020, June 24) Wrongfully Accused by an Algorithm . New York Times, retrieved from https://www.nytimes.com/2020/06/24/technology/facial-recognition- arrest.html?login=email&auth=login-email

[22] https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

[23] See T.C Sottek., J., Kopstein (July 17, 2013). Everything you need to know about PRISM. The Verge. Retrieved from http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet, Lee T., (June 12, 2013) Here's everything we know about PRISM to date. Washington Post. Retrieved from http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/, Edward Snowden Interview (July 08, 2013). The NSA and Its Willing Helpers. Spiegel online International. Retrieved April 22, 2014 from http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

What French sociologist Jacques Ellul worried about in 1954 has transpired: the police quest for unlimited information makes everyone a suspect. [24]

According to New York Times, China is already using surveillance technologies in order to identify and track billions of people.[25] The mere description of the surveillance network that China has developed raises serious concerns regarding the breach of fundamental human rights. It is part of a bigger plan, the so-called "Social Credit System" that even if not fully deployed it still remains an extended nationwide scheme "for tracking the trustworthiness of everyday citizens, corporations, and government officials''[26] The Chinese government sustains that the whole project is designed to boost public confidence and fight corruption and business fraud, but in the eyes of human rights and privacy advocates, China has created an intrusive surveillance apparatus to establish or rather reinforce the existing authoritarian state.

But even if in western democracies mass surveillance is theoretically constrained by the rule of law, that is not always the case. As the recent Clearview facial recognition technology case has revealed it is not just China that should be pointed to as the obvious culprit in surveillance discussion. A large number of law enforcement agencies in U.S.A have been using Clearview in order to have access to billions of persons' photos without consent and without transparent procedures.[27]

3.3 Privacy and data protection

Police forces use artificial intelligence systems to access and analyze data sets in order to prevent and predict crime. Artificial intelligence systems are fed with data that is collected by a vast number of combined data sources. The problem is that the data used in the course of predicting policing and surveillance and analysis of data by data mining methods and artificial intelligence systems reveals private information that qualifies as personal data[28] and in many cases sensitive information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[29]

The scale of surveillance in a dystopian future which actually happens right now is illustrated in report by the non governmental organization Access Now. [30] According to the Report "researchers have developed Machine Learning models that can "estimate a person's age, gender, occupation, and marital status just from their cell phone location data" as well as to"predict a person's future location from past history and the location data of personal data.[31] As the report describes there is a systematic and increased collection of social media information from law enforcement agencies that feed it to artificial intelligence -powered programs to detect alleged threats. The problem is that these programs not only target certain public social media activities but in reality "involve massive, unwarranted intake of the entire social media lifespan of an account"[32]

4. ETHICAL AND LEGAL GOVERNANCE

While the need to have effective law enforcement agencies is not a controversial subject, the unobstructed use of artificial intelligence by it raises serious concerns. The way to mitigate effective policing with the simultaneous respect for human rights is the creation of a regulatory framework and codes of conduct for the use of artificial intelligence by governments.

Many scholars and organizations are dealing especially with the use of artificial intelligence by law enforcements agencies advocating for a number of balancing measures.In 2019 the United Nations Interregional Crime and Justice Research Institute's (UNICRI), Centre for Artificial Intelligence (AI) and Robotics, and Innovation Centre of the International Criminal Police Organization (INTERPOL) published a report on "Artificial Intelligence and Robotics for Law Enforcement" .The report among others analyses the contribution AI and robotics in policing examines use cases at varying stages of development and makes a recommendations and suggestions for the ethical and legal use of AI and robotics in law enforcement.[33]

In particular the report states that in order for law enforcement agencies to respect citizen's fundamental rights and avoid potential liability, the use of AI and robotics in law enforcement should be characterized by four basic principles.

1. Fairness; decisions made are fair by not breaching the right to due process, presumption of innocence, the

[24] Lyon, D. (2020, Mely 24) The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy. The Conversation. Retrieved from https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060

[25] The title of the article alone is rather revealing . Mozur, P. (2018J, July 8) Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras. The New York Times. Retrieved from https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[26] Matsakis L. (2019, July 29) How the West Got China's Social Credit System Wrong.WIRED Magazine. Retrieved from https://www.wired.com/story/china-social-credit-score-system/

[27] Kashmir H. (18. January 2020) "The Secretive Company That Might End Privacy as We Know It" The New York Times. Retrieved from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[28] See Mitrou, L. Data Protection,. Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? (December 31, 2018). Retrieved from SSRN: https://ssrn.com/absurveillance form use of police artificial intelligence

stract=3386914 or http://dx.doi.org/10.2139/ssrn.3386914

[29] See Article 9 (1), Article 4 (14), (15) and recitals 51 to 56 of the Regulation (EU) 2016/679

[30] Access Now is an NGO working in the field on digital civil rights. See https://www.accessnow.org

[31] Access Now, 'Human Rights in the Age of Artificial Intelligence' (8 November 2018) Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

[32] ibid

[33] INTERPOL – UNICRI Report. (2019) "Artificial Intelligence and Robotics for Law Enforcement" Retrieved from http://www.unicri.it/news/files/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB.pdf

freedom of expression, and freedom from discrimination,

2. Accountability; law enforcement agencies should establish a culture of accountability at an institutional and organizational level,

3. Transparency; in order to avoid the so called 'black box' the should promote transparency in the path taken by the system to arrive at a certain conclusion and

4. Explainability; that is to establish a framework of explaining the decisions and actions of a systems must be comprehensible to human users.

5. CONCLUSIONS

As we are heading towards a future of widespread adoption of artificial intelligence technologies by many actors, it is becoming increasingly necessary to clearly define the data protection and privacy risks and the legal framework applicable in their use, even more so when law enforcement agencies are involved in the task.

Artificial intelligence may have been embraced and used in a variety of fields from health care to marketing, however it is the use of AI applications by the police which raises the most urgent issues since it is the misuse that threatens the very core of human rights; it is ,after all, the the police that can detain, arrest or even use deadly force when deemed necessary. [34]

It has been shown that many types of data available on a smart mobile device are considered as personal data. It has also been stressed that the main issues surrounding privacy problems within the "app" ecosystem lie in its fragmented nature and the wide range of technical access possibilities to data stored in or generated by mobile devices.

Recent unrest that followed the death of George Floyd illustrated in vivid colors that there is a significant trust deficit towards the police. The question remains, especially in the case of western democracies whose very foundations were laid on the rule of law, to achieve public safety without encouraging or tolerating the creation of a police state . The key here lies in the creation and coordination of an intertwined system of checks and balances supported by a complete set of rules aimed at the protection of the core of human rights and dignity that will bind both governments and law enforcement agencies, while at the same time establishing a sense of security and trust amongst the population.

[34] Joh, E.E., Artificial Intelligence and Policing: First Questions (April 25, 2018). 41 Seattle Univ. L. Rev. 1139 (2018). Available at SSRN: hhttps://ssrn.com/abstract+316879