Total ban or responsible use?
A policy survey to better regulate the use of AI-powered video surveillance in law enforcement in the European Union

July 2022

Glasgow Student Number: 2572578R

Trento Student Number: 225064

Charles Student Number: 59656761

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 21894

Supervisor: Dr Petr Špelda (Charles University)

Date of Submission: 25/07/2022

Acknowledgements

I dedicate this work to Henri Ceccon, my beloved grandfather and guardian angel. I will always carry with me your values of humanity, humility, determination, passion and hard work. I miss you.

I would firstly like to thank my supervisor, Dr Petr Špelda, for his guidance, flexibility, and availability throughout this process. His expertise in technologies and particularly in artificial intelligence was essential to accurately address this topic.

I would also like to thank all my family, especially my parents Sandrine and Nicolas Rolland for their constant support, their listening, and their love. They best taught me the importance of nuance that I have tried to convey in this work.

I am grateful to Pauline Massart for her support and trust, for taking me into her team while allowing me to dissertation my thesis in the best conditions.

I thank Marine Adamson, Marie Ketterlin, Juliana Matallana and Florence Warren for their continuous moral support and feedback throughout this process. I could not have asked for a better environment to write this dissertation. Thank you for being such great friends.

I would also like to thank all my IMSISS classmates for these two great years and the fantastic environment we created. I am proud of us for going through this master at such a special time. In particular, I would like to thank Mara Thurnhofer, my partner in crime in this master and salute our ability to keep pushing for what we believe in. A special thought also to Delphine Debuire, Joachim Sarfati, Marine Krauzman, Sarah Adam, Johanna Broquet, Alessia Borg, Clara Stejksalova, Emma Bicknese, and Minalè Nouri for listening to my (many) grievances. Finally, I would like to thank the IMSISS consortium for trusting me with a scholarship, without which I would not have been able to pursue this master so serenely.

To conclude, I would like to thank Marco Farucci for his constant support and feedback during this process, and also in the everyday life. Thank you for taking the time to read me over, advise me and always cheer me up.

Table of Contents

List of Tables

Abstract

AI-powered video surveillance is a heated issue in the European Union which has given rise to a very polarised debate. On the one hand, proponents advocate for its ability to make cities safer and better protect people. On the other hand, opponents are concerned about the technology's threat to fundamental rights and individual freedoms, such as the right to privacy or fear of the risk of discrimination. European institutions have started attempts at regulating the technology but have so far been struggling with the development of a broad regulation that accounts for the diversity of applications found in AI-powered video surveillance, protects citizens, and encourages innovation at the same time. This dissertation therefore investigates how to implement responsible use of AI-powered video surveillance for predictive policing purposes. To do so, the analysis is divided into two parts which correspond to the two main branches of application of AI-powered video surveillance: object-centred and person-centred AI-powered video surveillance. It first uses securitisation theory to situate the debate. Next, it uses Document Analysis and coding to analyse the qualitative data. The qualitative data encompasses policy and technical documents to allow for a nuanced approach to the issue that accounts for the actual capabilities and limitations of the technology. For each of these case studies, the author looks at the opportunities and challenges of the application of the technology. Opportunities include technical capabilities as well as positive implications to better protect citizens. Challenges include technical limitations as well as negative implications for human rights. Understanding the opportunities and challenges of AI-powered video surveillance is a necessary step toward the development of adequate and proportionate regulation. They are also used to develop a roadmap for responsible use of AI-powered video surveillance.

Finally, this dissertation argues for the need to challenge the wider system in which AI-powered video surveillance is embedded to implement responsible

use of the technology. It claims that the debate should also look beyond the technology itself and question current crime prevention and predictive policing practices. The latter is focused on the notion of pre-crime, the belief that law enforcement should work towards the reduction and elimination of crime rather than responding and investigating it. Such an approach is characteristic of the risk society in which we live, a model of society obsessed with the control of risk rather than of harm. Thus, current crime prevention practices are embedded in policing practices, sometimes to the detriment of more sustainable and long-term solutions based on broader socio-economic policies. The responsible development of the technology cannot be done without considering alternative options that may be more appropriate.

Chapter 1: Introduction

The use of AI-powered video surveillance for predictive policing by law enforcement agencies is a particularly heated issue in the European Union (EU) at the moment. AI-powered video surveillance refers to the integration of artificial intelligence (AI), and more precisely machine learning (ML) algorithms in video surveillance camera systems. Algorithms process large amounts of visual data through pattern recognition to detect and track entities and flag abnormal events to law enforcement. It allows law enforcement agencies to predict crimes, to allow officers to act pre-emptively and improve crime prevention.

The first part of this introduction gives a brief overview of the history of AI-powered video surveillance to better understand the context and policing practices in which it emerged. Then, it highlights the current debate surrounding the use of the technology and defines the current position of the EU on the matter. Next, it details the research question and initial assumption of the research. Finally, it outlines the different chapters of this research that allow to tackle the issue.

AI-powered video surveillance is a product of the wider proliferation of surveillance and innovation in technologies, supported by the rise of data analytics.

The Second World War triggered the development of domestic mass surveillance, which continued to slowly develop during the Cold War and has grown exponentially since the fall of the Berlin Wall. From then on, Cold War military technologies were repurposed in the West for law enforcement uses, giving them extensive surveillance power (Milligan, 1999). This led to the emergence of the 'surveillance society'. Surveillance societies are societies that partly operate through the large-scale collection and processing of information about individuals in their daily lives (Lyon, 1994). Furthermore, the changing

nature of the security threat environment has also contributed to the development of the surveillance society. In an increasingly globalised world, threats have become transnational and intrastate, such as organised crime and terrorism (McCahill, 2008). In particular, terrorism has led to the intensification of surveillance in the West (McCahill, 2008). The September 11, 2001 attacks in the United States (US) and subsequent terrorist attacks across the West have given rise to a war on terrorism[1], which involved taking significant security measures to prevent terrorism (Milligan, 1999). The war on terror contributed to providing law enforcement agencies with extensive surveillance powers to monitor public spaces. As a result, surveillance in cities has gradually become a characteristic and a requirement of modern life, a kind of surveillance driven by a precautionary principle and a desire to control all risks (Delbecque, 2015).

The increase in surveillance has also been supported by technological developments. The quality of cameras has improved and camera networks have proliferated drastically around the world over the last twenty years (Abdulghafoor and Abdullah, 2022). In addition, the rise of Big Data, the processing of large datasets by software, has revolutionised surveillance. In particular, AI, the ability of machines to perform human-like skills, and ML, a branch of AI that makes predictions and adapts to changing environments without being explicitly programmed to do so, have had a fundamental impact on surveillance in cities (Joshi, 2020). The ability to process large amounts of data has given rise to predictive policing, a data-driven crime prevention practice that allows law enforcement to rely on algorithms to process large amounts of data through pattern recognition to better predict and prevent crime (Egbert and Leese, 2020). Predictive policing is part of a broader system of crime prevention that has moved towards the notion of pre-crime, the idea that law enforcement should focus on reducing and eliminating crime *before* it occurs, rather than reacting and investigating crimes *after* they have occurred

[1] Also known as 'war on terror'.

(Asaro, 2019). This development is a direct result of the emergence of the 'risk society', a model of society obsessed with the control of risk rather than of harm, which has been promoting pre-emptive policing measures to combat crime since the late 20th century (Beck, 1986; Strikwerda, 2021).

This revolution has also occurred in video surveillance, where ML algorithms were integrated into cameras to enable video analytics. Remote video surveillance is a traditionally time-consuming and human-error-prone activity that offers limited results for the prevention of crime. However, ML algorithms gave users the ability to process unprecedented amounts of visual data through pattern recognition to detect, recognise and track entities in real-time and more efficiently. Video surveillance has thus moved from being a passive and reactive technology, whose main interest was to be used in post-crime situations, towards becoming an active technology that can be used to prevent crime (Lindsey and Woolf, 2021). This ability to spot abnormal events through visual recognition has allowed video surveillance to become a tool of predictive policing.

However, the use of AI-powered video surveillance for predictive policing has sparked a very heated and polarised debate within the EU. On the one hand, governments, and law enforcement agencies, largely supported by private security actors who develop these technologies, highlight the ability of AI-powered video surveillance to better predict and prevent crime to protect citizens. On the other hand, data rights and privacy advocates have called for a moratorium or ban on the technology, particularly facial recognition, due to concerns about the technology's impacts on human rights, such as the threat to privacy and the risk of discrimination.

Meanwhile, European institutions have started attempts at regulating the use of AI-powered video surveillance. Specifically, they have been working on the AI Act (2021), a legislation that proposes a risk-based approach to regulating AI more generally. As a result, live facial recognition could become prohibited.

However, the current draft does not provide adequate guidance, with clear procedures and safeguards, for the wider uses of AI in video surveillance, such as object-centred surveillance. The EU also fails at clearly stating its position, with the different institutions voicing different opinions on the matter. For example, the European Commission advocates a cautious use of facial recognition technology, while the European Data Protection Supervisor (EDPS) has called for a complete ban and the European Parliament promotes a moratorium (Ragazzi et al., 2021). At the same time, the European Parliament has also recently granted Europol, the EU law enforcement agency, extended powers to use AI for policing purposes (Bertuzzi, 2021).

The technology offers promising possibilities to better fight crime and protect individuals, which by extension would also have a positive impact on human rights. However, it also poses significant challenges that, if left unaddressed, will undermine human rights and individual freedoms. This dissertation therefore explores how AI-powered video surveillance for predictive policing can be implemented responsibly, if at all.

The initial assumption of the research is that responsible use could be achieved if the opportunities and challenges of the technology are better understood and considered by policymakers. A ban on the technology is not currently deemed a viable option, as it could prevent the possibility of innovation and improvement of the technology to match EU values. On the contrary, a ban could lead to the EU losing its normative power to other powers that continue to develop and deploy AI-powered video surveillance on a global scale and do not share the same human rights standards.

To understand how to develop a responsible use of AI-powered video surveillance in the EU, this dissertation puts forward a realistic approach which considers the actual possibilities offered by the technology. It argues for the necessity to understand its technical capabilities and limitations to better understand its positive and negative implications. At present, European

policymakers are struggling to grasp the capabilities of the technology, although this should be the guiding principle for any regulatory development. The author therefore aims to provide a better understanding of some of the applications of AI in video surveillance, namely object-centred and person-centred AI-powered video surveillance, to provide a roadmap for responsible use of the technology by law enforcement for predictive policing.

To investigate how AI-powered video surveillance can be implemented responsibly, this dissertation is divided into six chapters, of which this introduction is the first.

In Chapter 2, the literature review first provides an overview of securitisation theory which is used as a starting point for the analysis in order to understand the debate surrounding the use of AI-powered video surveillance. The second part of the literature review looks at the wider practices of crime prevention and predictive policing, in which AI-powered video surveillance is embedded. Finally, it examines the literature on the opportunities and challenges of predictive policing and ML models in the context of AI-powered video surveillance, to lay the groundwork for a nuanced approach that considers the capabilities and limitations of the technologies for a better understanding of the implications of the technology.

In Chapter 3, the research design and methodology chapter explain and justify the research methods chosen. The selected case studies are the two main branches of AI-powered video surveillance: object-centred and person-centred AI-powered video surveillance. The analysis relies on securitisation theory as a starting point to situate the public debate. Then, Document Analysis and coding are used to analyse the data, which originate from policy and technical documents to allow for a nuanced approach. The author uses an inductive approach to establish the opportunities and challenges of each branch of application, which allows the establishment of a roadmap for responsible use of AI-powered video surveillance.

Chapter 4 provides the analysis of the data through object-centred and person-centred AI-powered video surveillance. The case studies are constructed similarly, starting with a presentation of the data analysed. It then looks at the securitisation of the application in the public debate. Next, it explores the opportunities and challenges offered by the technology, considering its technical capabilities and limitations, and its positive and negative implications.

Chapter 5 presents a discussion of the main findings. Firstly, it sets out a roadmap for the responsible use of AI-powered video surveillance. Secondly, it challenges the current system in which AI-powered video surveillance is embedded, arguing that responsible use of the technology also involves questioning current practices of crime prevention and predictive policing.

Finally, Chapter 6 presents the conclusion of this research.

Chapter 2: Literature Review

The current debate around the use of AI-powered video surveillance is rooted in rhetoric. The first part of this literature review provides a brief overview of securitisation theory to show how proponents and opponents frame the issue and polarise the debate.

As this dissertation argues that it is necessary to move beyond rhetoric, the second part of the literature review examines the wider policing practices in which AI-powered video surveillance is embedded. Indeed, much of the debate about the technology actually stems from the practice of predictive policing, of which AI-powered video surveillance is an application.

Finally, the last part of the literature review focuses on the opportunities and challenges of predictive policing and ML models in the context of AI-powered video surveillance. This allows this dissertation to take a nuanced approach that considers the actual capabilities and limitations of the technology, in order to better regulate it.

Securitising AI-powered video surveillance

Much of the current debate on the use of AI-powered video surveillance stems from the securitisation of the technology in public discourse. A brief introduction to the theory of securitisation is therefore given, before identifying the different actors and objects of securitisation on both sides of the debate.

Broadly conceived, securitisation refers to a process whereby actors, usually state actors, transform ordinary political issues into security issues enabling them to use extraordinary means in the name of security (Buzan et al., 1998). Securitization theory was introduced by the Copenhagen School (CS), a school of thought that challenges traditional security studies by focusing on the

non-military aspects of security. CS emphasises speech act analysis to explain how securitisation works (Rychnovska, 2014). It argues that securitisation involves a securitising actor performing a securitising move through a speech act on a given audience, who must accept the move (Hanse et al., 2011; Bourbeau, 2015). Consequently, an issue does not need to be real to be securitised, instead, the discourse that frames it is more relevant (Balzacq, 2005). Here, securitisation is rooted in a logic of exception which turns a phenomenon into an existential threat that requires exceptional measures to be taken by security actors to be countered (Vultee, 2010; Bourbeau, 2015).

Critics of CS challenge its over-focus on speech act, finding its approach objectivist, focused on static elements and restrictive for empirical research (Stritzel, 2007). Critics defend the importance of considering context to understand securitisation, which they find rooted in a logic of routine (Bourbeau 2015). Here, an issue becomes securitised through routinised practices which go beyond speech act. Nevertheless, they also agree that an issue does not have to be real to be securitised. Accordingly, Stritzel (2007) argues that a securitised issue is the product of a negotiation between securitising agents and the securitised audience.

In the case of AI-powered video surveillance, there are two distinct securitising actors and securitised objects to justify the adoption of two different sets of exceptional measures.

On the one hand, the proponents of AI-powered video surveillance, embodied by law enforcement and governments, largely supported by the private companies that sell the technology (actors), securitise the threat environment (object) to justify the use of the technology (exceptional measure). Since the September 11 terrorist attacks in the US and the subsequent war on terror, the concept of 'threat environment' has been widely leveraged as a political tool to legitimate the enactment of exceptional measures to protect citizens (Romaniuk and Webb, 2015). In the context of AI-powered video surveillance, the 'threat environment' refers to the various threats of a criminal nature that can be found

in cities, from incivilities to theft, violence or assault, which justifies the actors' desire to predict crime to better prevent it.
On the other hand, opponents of AI-powered video surveillance, with data rights and privacy advocates, NGOs, and activists (actors), securitise the technology itself (object) to justify the need to ban it (exceptional measure).

AI-powered video surveillance has therefore been securitised, although there is no academic literature on this specific issue at the time of writing this dissertation. The latter aims to go beyond the rhetoric, to understand the reality behind the framings proposed by the various actors in the debate and grasp what the technology can actually do. Thus, the following section provides a better understanding of the context in which the use of AI-powered video surveillance has emerged, namely crime prevention, and more specifically predictive policing.

From crime prevention to predictive policing

Crime prevention designates "[practices] shown to result in less crime than would occur without the practice" (Sherman et al., 1998, p.2). Crime prevention is conducted by actors beyond law enforcement, such as social workers, communities, and schools (Sherman et al., 1998). This literature review, however, focuses on crime prevention conducted by law enforcement. According to Egbert and Leese (2020), crime prevention is a long-standing practice, as the police have always sought to prevent criminality by examining patterns of crime occurrence to estimate potential future criminal trends, rather than investigating only the crimes that have been committed. However, the digital age has completely revolutionised crime prevention as digitisation allows for the continuous production of unprecedented amounts of data, nearly unlimited storage capacity and processing power, and new methods of extracting information from datasets (Egbert and Leese, 2020). Powerful IT systems in the 1990s allowed police officers to become "knowledge workers"

with “a managerial [role] supposed to assemble intelligence in order to administer threat” (Egbert and Leese, 2020, p.20). Data enabled the emergence of new capabilities in law enforcement, particularly concerning engagement and management of the future, with the idea that big data mining could provide new insights and improve crime prediction (Egbert and Leese, 2020). This development has been supported by two phenomena: the “scientification of police work” and the “turn toward digital futures”, with the growing desire to prevent adverse events before they occur (Egbert and Leese, 2020, p.21). First, the scientification of police work refers to the increasing use of advanced statistical models and academic theories in law enforcement work, supported by technological innovations and the growth of information and communication technology (ICT) (Egbert and Leese, 2020). Second, the turn to digital futures has seen a reorientation of crime processes toward future threats with the emergence of notions of ‘pre-crime’ (Asaro, 2019; Egbert and Leese, 2020). Strikwerda (2021) describes a shift from a post-crime to a pre-crime model, in which ordering practices are preventive, with law enforcement models moving from threat mitigation to threat anticipation. Crime fighting first took a ‘preventive turn’ (Crawford and Evans, 2012, p.798) in the US in the 1970s and 1980s, as the country faced a rise in criminality. It was politically motivated according to Egberts and Leese (2021), stemming from a political decision to bring crime levels down. This trend accelerated after the attacks of September 11, 2001, with the advent of a ‘risk society’ obsessed with crime prevention and the control of risk rather than that of harm (Beck, 1986; Strikwerda, 2021).

The practice of predictive policing emerged in this context, inscribed in larger trajectories of crime prevention strategies. Predictive policing is motivated by the same logic that explains why law enforcement agencies use technology: for practical reasons, with new capabilities and modes of action; for political and managerial reasons, as an opportunity to address shortcomings and failures in policing and increase efficiency; and to professionalise the police as an organisation (Egberts and Leese, 2021). Predictive policing came from a

desire to actively shape the future, but also from political and public pressure to lower crime levels as well as economic pressure of rendering police work more efficient and effective through a better allocation of resources (Egberts and Leese, 2021). Furthermore, predictive policing was supported by the rise of Big Data and the information society in the 2000s and the development and use of technical means for systematic data analysis by law enforcement (Egberts and Leese, 2021). ML models achieved to revolutionise the practice of predictive policing, enabling law enforcement users to process unprecedented amounts of data through pattern recognition and improve crime prediction and prevention (Kaufmann, Egbert and Leese, 2019).

Defining predictive policing

Predictive policing was coined in 2008 in the academic literature, referring to "data-driven, risk-oriented approaches to police operations" (Egberts and Leese, 2021, p.27). It relies on large amounts of data and sophisticated algorithms and has been facilitated by a rapidly increasing storage capacity and computing power (Egbert and Leese, 2020). Broadly conceived, predictive policing simply refers to the ability of law enforcement agencies to predict crime using algorithms capable of processing large amounts of data through pattern recognition. In the academic literature, however, a clear definition of predictive policing is lacking, although the concept has been the subject of much research. Nonetheless, researchers agree on certain characteristics, described in the following paragraphs.

The first characteristic of predictive policing is the desire to predict crime through pattern recognition in data analysis. Moses and Chan (2018) define predictive policing as a "term applied to a range of analytical tools and law enforcement practices" with a supposed ability to predict crime "combined with changes in law enforcement decision-making [...] based on these forecasts" (p.806). Analytical tools involve the use of algorithmic software to predict

where, when and by whom a crime will be committed (Moses and Chan, 2018). Such software can identify patterns that provide information about regular occurrences of crime in datasets that are otherwise difficult or impossible to detect by a human agent (Kaufmann, Egbert and Leese, 2019). The models provide spatial and temporal indications of the distribution of crime, which shape knowledge about "regular occurrences of crimes that lie hidden in datasets" (Kaufmann, Egbert and Leese, 2019, p.674). Predictive policing software is based on ML models, a branch of AI that is a method of automated data analysis that assumes that systems can learn from data, discover patterns and make predictions with little human interaction (Koza et al., 1996). ML is said to be 'supervised' when humans annotate the datasets and supervise how the system learns, 'unsupervised' when the system itself aggregates the data, or 'semi-supervised' when only a portion of the data is labelled (Ragazzi et al., 2021). ML models are built from training data, i.e. samples of data from the surrounding environment used to make predictions and decisions (El Naqa and Murphy, 2015). Algorithms thus enjoy 'considerable authority' (p.674) according to Kaufmann, Egbert and Leese (2019): they are designed and deployed for specific purposes of crime prediction, help to make sense of unintelligible datasets, and provide the "epistemic foundation for data-driven analyses" (p.674). More specifically, Meijer and Wessels (2019) describe predictive policing as the collection and analysis of past crime data to identify and make statistical predictions about 'at-risk' individuals and locations with a higher likelihood of criminal activity to implement police strategies and techniques to prevent crime.

The second key characteristic is the belief and desire that crimes can be prevented based on the predictions through the adoption of policing strategies and tactics. Meijer and Wessels (2019) explain that predictive policing is based on the idea that policing can be 'pre-emptive' (p.1033), the notion that law enforcement officials can act before criminal activity occurs. Similarly, Uchida (2009) and Norton (2013) claim that predictive policing assumes that crime can

be predicted using data analytics, while Egbert and Leese (2021) argue that it offers estimates of possible futures as a basis for developing adaptable operational policing measures. Moses and Chan (2018) argue that law enforcement may prevent crime by adopting a proactive response and basing its decision-making on algorithmic predictions, with the adoption of preventive strategies such as the deployment of police personnel. Thus, for Leese (2021), predictive policing "[reinforces] the trend towards future-oriented knowledge and action" in the security field (p.151), while Perry et al. (2013) describe predictive policing as a cycle of activities and decision points that includes data gathering, analysis, police actions, criminal reaction, and return to data collecting.

Nevertheless, even if scholars agree on key features, Egbert and Leese (2021) argue that predictive policing cannot be considered a unique phenomenon. Although Egbert and Leese (2021) agree on the general idea that predictive policing involves the use of algorithms to detect patterns in large datasets to predict and prevent crime, they explain that several models, processes, algorithms and software applications exist to perform predictive policing. The applications of predictive policing depend greatly on the desired outcome, such as the type of crimes targeted ranging from burglary to gang violence (Egbert and Leese, 2020). However, predictive policing is not limited to predicting the crime itself, it can also be applied to predicting potential victims. Perry et al. (2013) divide predictive policing methods into four categories (p.8):

- "Methods for predicting crimes", forecasting places and times where crime is likely to occur
- "Methods for predicting offenders", identifying individuals at risk of committing a crime in the future
- "Methods for predicting perpetrators' identities", creating profiles that match likely offenders with specific past crimes

- "Methods for predicting victims of crimes", identifying groups likely to become victims.

Traditionally, predictive policing can be either person-based or place-based. Person-based predictive policing seeks to identify 'at-risk' individuals, such as potential perpetrators or victims and can include risk-profiling or social network approaches (Asaro, 2019; Egbert and Leese, 2020). The former aims at identifying who is likely to become a perpetrator or a victim, while the latter assesses risk according to the social contacts of an individual. Meanwhile, place-based predictive policing aims at identifying 'at-risk' geographical areas where crime is likely to occur (Asaro, 2019; Egbert and Leese, 2020).

This brings to a final important element of predictive policing concerning the data itself and the means and tools to collect it. First, scholars agree that a large amount of data is needed for predictive policing. Meijer and Wessels (2019) emphasise "the usage of a broad variety of sorts of data" to conduct predictive policing, while Leese (2021) argues that predictive policing actually "[thrives] on the availability of data" (p.151). Kaufmann, Egbert and Leese (2019) explain that the belief that large amounts of data are sufficient to better predict the world is embedded in broader narratives of Big Data and data mining.

As there are many ways to conduct predictive policing, the type of data input into algorithms depends on the goal that law enforcement wants to achieve. Most academic literature emphasises the use of historical and criminal data as the main data sources for predictive policing, but predictive policing can exploit other types of data depending on the targeted crime to be tackled, such as social media, mortgage defaults, traffic, etc. (Moses and Chan, 2018; Meijer and Wessels, 2019; Egbert and Leese, 2020). Law enforcement agencies often work with data generated by themselves or from secondary sources such as public administrations or commercial data purchased from private companies (Kaufmann, Egbert and Leese, 2019).

Similarly, the predictive policing tools and techniques used also depend on the desired outcome for law enforcement. These tools range from risk assessment algorithms to social media monitoring and video surveillance, again offering a variety of data sources that can be combined for increased performance (Moses and Chan, 2018). In that, Egbert and Leese (2021) conceive predictive policing as a scientific method that mobilises criminal theories and empirical knowledge about crime.

Therefore, there are many ways to practice predictive policing. Visual data is one of many different data sources that can be used to develop predictive policing software, with computer programs that allow real-time video analysis to better predict and prevent crime using pattern recognition to analyse visual data. However, in the academic literature, AI-powered video surveillance is largely ignored in the field of predictive policing. This dissertation therefore adopts a broad understanding of predictive policing: the use of a large amount of any type of data to find patterns to better predict and prevent crime. It considers AI-powered video surveillance and its different applications, such as object recognition or facial recognition, as one way of doing predictive policing since it processes large amounts of visual data to predict and identify threats. ML models have revolutionised video surveillance to become a proactive technology, thereby suitable for predictive policing purposes. Video surveillance was originally reactive, focused on understanding crime after it had occurred rather than preventing it. Although law enforcement officers continuously watched videotapes to identify abnormal and suspicious activity, the ability to prevent crime using video surveillance was rather limited as this effort is time-consuming, detail-oriented, prone to human fatigue and bias. The use of ML models now allows to monitor a given scene in real-time and take proactive action to prevent crime.

Opportunities and challenges in predictive policing software used for video surveillance

This next part of the literature review focuses on the challenges and opportunities posed by predictive policing software which apply to AI-powered video surveillance to lay the bases of the analysis.

Opportunities

Predictive policing aims to provide law enforcement with situational awareness to respond more quickly and effectively to criminal activity, better allocate resources and increase efficiency. This section examines the opportunities of predictive policing, specifically as applied to AI-powered video surveillance.

Proponents of predictive policing point to its ability to reduce crime and improve safety in cities, as Mohler et al. (2015) and Ariel (2019) note in their work. Proponents argue that predictive policing allows for a better allocation of resources (Schlehahn et al., 2015; Meijer and Wessels, 2019). Indeed, it allows the processing of unprecedented amounts of data and provides information that would be humanly impossible to obtain (Kaufmann, Egbert and Leese, 2019). By automating police work, predictive policing relieves officers of the burden of analysis and allows them to focus on other tasks, based on accurate information provided by the software (Leese, 2021). This allows for a more targeted deployment of law enforcement resources in time and place and makes predictive policing a more effective and efficient policing method (Meijer and Wessels, 2019). According to Raajmakers (2019) and Jenkins and Purves (2020), the use of AI in predictive policing makes law enforcement work faster and more cost-effective. These cost-efficiency arguments apply to AI-powered video surveillance since the data compiled by the video analysis makes it possible to better identify places and individuals at risk (Barroca, 2021; Kwet, 2020). Video surveillance is a difficult task for human agents, as their ability to monitor a given space in real-time while analysing and reacting to threats, is

extremely limited. AI-powered video surveillance therefore allows for real-time, faster analysis that enables law enforcement to react more quickly. It turns video surveillance into a proactive technology able to prevent crime rather than a reactive technology only used to analyse a crime scene after a crime already occurred (Lindsey and Woolf, 2021).

Furthermore, proponents of predictive policing argue that algorithms are less prone to error than humans. They argue that humans are likely to make many mistakes, either because they are distracted, tired or because of a lack of skill (Egbert and Leese, 2020). According to these proponents, this is not the case with algorithms, which they argue are more accurate than humans due to their data-driven nature (Browning and Arrigo, 2020). Specifically with video surveillance, Lindsey and Woolf (2021) argue that AI can create intelligent systems that can better focus on specific security objectives by removing noise in the environment, widening the field of view and increasing flexibility. They also claim that AI-powered systems significantly reduce the number of false positives, making their analysis more accurate and reliable than humans'.

Finally, proponents of predictive policing argue that algorithms are less biased than humans. They claim that just as humans are inherently biased, so too are law enforcement analyses. Human cognitive biases would influence decision-making and systematically lead to biased results. In contrast, algorithms would be unbiased, neutral and impartial, offering opportunities to overcome human bias and provide more equitable results (Egbert and Leese, 2020). This argument can also be found in the academic literature in favour of AI-powered video surveillance, notably by proponents of facial recognition who consider that algorithms can overcome human racial bias, although this view is also widely disputed.

Predictive policing is said to be more cost-effective, more accurate and more reliable and therefore superior to error-prone human analysis. This argument is part of a broader narrative that invokes science as the sacrosanct solution and

believes in a kind of 'technological solutionism', the belief that technology can solve all problems (Bigo, 2020). However, the actual effectiveness of predictive policing in reducing crime remains to be confirmed, with Meijer and Wessels (2019) highlighting a lack of empirical evidence. It is true, for instance, that AI-powered video surveillance has promising applications for the recognition of visual data, such as the recognition of objects, license plates, faces, events, abnormal behaviour and even emotions, among others (Kwet, 2020). However, the practice of predictive policing and the applications of AI-powered video surveillance have been subject to multiple criticisms in the academic literature, explained in the next section.

Challenges

Critics of predictive policing argue that it is based on false assumptions derived from a lack of understanding of what software can actually do. Many of these limitations have to do with that of ML models used in predictive policing software. The next paragraph provides a literature review on the intrinsic issues of predictive policing software and ML models, with the perspective of AI-powered video surveillance.

Critics first argue that predictive policing does not address the root causes of crime, but only its symptoms. Moses and Chan (2018) explain that predictive policing assumes that the future will be the same as the past, and Egbert and Leese (2021) point out that the practice relies on historical data rather than live data, allowing only a retrospective analysis of criminal behaviour. They further argue that it is a reactionary technology designed to identify correlations, an argument shared by Meijer and Wessels (2019) who consider this focus excessive. The latter also highlights a lack of empirical evidence to assess predictive policing technologies' ability to reduce crime effectively (Meijer and Wessels, 2019). These criticisms are highly relevant to AI-powered

video surveillance, as this technology does not address the root causes of crime, but rather offers a short-term solution to prevent imminent crime.

The second set of criticisms concerns the data itself. Predictive policing algorithms are supposed to provide an accurate representation of reality by searching for patterns of crime in large datasets, yet this is not the case (Moses and Chan, 2018). Data is subject to errors: it may be incomplete, wrongly entered or overlooked (Leese, 2020; Egbert and Leese, 2020). Crime data are particularly known to be partial and unreliable and change throughout investigations, requiring frequent updates that are not always made (Leese, 2020). Thus, data is a partial representation of reality and reflects the observations of an individual working for a particular purpose and in a particular context (Leese, 2020). ML models remove this context and offer a skewed version of reality (Meijer and Wessels, 2019).

Data is also subject to selection bias and is inherently inaccurate and biased (Browning and Arrigo, 2020; Leese, 2020). Policing is a historically biased practice and police data is subject to geographical, political and social biases (Schlehahn et al., 2015; Browning and Arrigo, 2020). Historical crime data is particularly prone to selection bias, as some of the data collected comes from periods when police practices were discriminatory. For example, there is an overrepresentation of 'street crime', such as robberies or drug dealing, in comparison to 'white-collar crime', such as corporate fraud or embezzlement. Some criminal data, such as domestic abuse, even goes unreported and is undetected in datasets, creating data gaps which further distort reality (Egbert and Leese, 2020; Buil-Gil et al., 2021). This creates a criminal type that does not fit the reality and leads neighbourhoods associated with street crime to be overrepresented in datasets and over-policed with increased police patrols and identity checks (Access Now, 2018; Asaro, 2019; European Union Agency for Fundamental Rights, 2020).

Data errors lead to biases in predictions and misjudgements in law enforcement decision-making, which reinforces prejudice and stigmatisation of some

communities. It leads to their over-policing, promotes discriminatory policing practices and exacerbates inequalities. However, Meijer and Wessels (2019) point to the lack of empirical evidence to assess the risk of increased discrimination, while Yen and Hung (2021) argue that it is ridiculous to expect algorithms to correct prejudices that society itself constantly reproduces. For them, the fault lies with the system in which the algorithms operate rather than with the algorithms themselves. In that, according to Egbert and Leese (2020), predictive policing algorithms may not be the ones producing bias but surely reproduce and perpetuate it.

The ability of the algorithms themselves to correct these biases is also disputed. Sandhu and Fussey (2021) question the ability of ML models used for predictive policing to eliminate bias and subjective error. Predictive policing software only do what they are taught to do and perceive the world through the data they are fed, hereby limiting their ability to correct bias (Kaufmann, Egbert and Leese, 2019; Egbert and Leese, 2020). Such an issue is prominent with AI-powered video surveillance. For example, Garvie and Frankle (2016) explain that facial recognition is significantly less accurate for people of colour and women than for white men, because training datasets feature white men predominantly. Algorithms reproduce biases in datasets, they are not neutral according to critics of predictive policing. Many argue that this problem also stems from an inability to find a universal definition and evaluation of the concept of fairness in the ML community which makes it difficult to develop adequate standards (Sylvester and Raff, 2018; Green and Hu, 2018).

Modelling allows for a simplification of reality, which reduces complexity but can lead to errors due to technical challenges inherent in ML models. Some prominent ones for AI-powered video surveillance are generalisation and classification issues. Generalisation refers to the ability of a model to adapt and process new data adequately to generate an accurate prediction (Mohri and Talwalkar, 2018). ML models struggle to adapt to new

and previously unseen data, especially if the data has undergone a distribution shift, i.e. the input data is different in the live environment from what it was in the training environment (Mohri and Talwalkar, 2018). Shifts in distributions in unpredictable environments therefore lead to errors (Mohri and Talwalkar, 2018). These include classification errors. Classification is a model's ability to classify new observations into categories based on its training data (Kotsiantis, 2007). It is a prominent issue in AI-powered video surveillance, as visual data is particularly shifting and unstable. This makes the deployment of ML models for visual recognition particularly challenging, as the above example of facial recognition difficulties due to the predominance of white males in training datasets shows.

Moreover, predictive policing algorithms raise important concerns around transparency and accountability. They rely on opaque and complex ML models that have been described as 'black boxes', as experts themselves cannot always explain how they work and formulate decisions (Meijer and Wessels, 2019; Couchman, 2019; Egbert and Leese, 2020). Additionally, the software is usually owned by private companies that are not required to disclose their codes, which further hinders transparency (Busuioc, 2021; Egbert and Leese, 2020). The lack of transparency makes access to information difficult, prevents the auditing of algorithms and leads to a lack of explicability, which is crucial for law enforcement to legitimise their actions and be held accountable (Asaro, 2019; Meijer and Wessels, 2019; Busuioc, 2021). Indeed, according to Busuioc (2021), more than transparency, law enforcement decisions must be explicable and verifiable to achieve accountability. Yen and Hung (2021) also support this argument and state that it is more important to understand *why* the algorithm is used and whether it serves its purpose, rather than *how* it exactly works to achieve transparency in explanation. Finally, this lack of transparency and accountability hampers trust between citizens and their government and undermines fundamental rights such as the right to privacy (Meijer and Wessels, 2019). Thus, according to Egbert and Leese (2020), predictive policing creates

a culture of suspicion and fosters a culture of mass surveillance while Amodei et al. (2016) stress the importance of protecting sensitive data used in ML models. These challenges are particularly tangible with AI-powered video surveillance due to the direct exposure to the camera and the sensitivity of visual data, such as biometric data.

The last criticism relates to surveillance avoidance, a major challenge of AI-powered video surveillance. Surveillance avoidance refers to the ability to avoid being monitored, as seen in the Hong Kong protests, where protesters avoided facial recognition tools by hiding their faces (Mahtani and Hassan, 2019), or in the Black Lives Matter protests (Doffman, 2020), where protesters turned off their phones to prevent law enforcement from accessing their location data. Indeed, even if law enforcement was able to develop an ethical and bulletproof video surveillance system, the issue of video surveillance would still arise. At a more technical level, surveillance avoidance is a robustness issue. In the field of ML, robustness refers to the ability of a model to deal with erroneous inputs so as not to be fooled during execution (Fernandez et al., 2005). ML models are developed in benign environments during the training and evaluation phases of the algorithms (Goodfellow et al., 2018). Benign environments are environments in which there are no adversaries, which can be defined as misleading inputs that aim to deceive the ML models, for example to deceive the classifiers (Kurakin et al., 2017). When ML models are deployed in non-benign environments, they may encounter adversaries (Goodfellow et al., 2018). As mentioned earlier in this literature review, ML models do what they are trained and tested to do, and they struggle to adapt to novel data in unpredictable situations. Surveillance avoidance therefore exploits this vulnerability of ML models and undermines the utility of using AI-powered video surveillance in the first place as it can be fooled. However, this issue remains largely ignored in the academic literature, especially when discussing visual recognition applications other than facial recognition.

Conclusion

This literature review provides an overview of the main considerations for regulating the use of AI-powered video surveillance. It shows that the current public debate is rooted in rhetoric, with both sides engaging in a securitisation process to justify the enactment of exceptional measures. It further demonstrates that much of the debate stems from issues with wider crime prevention practices, in particular predictive policing. The literature review lays the groundwork for understanding the current state of opportunities and challenges for predictive policing in relation to AI-powered video surveillance. These opportunities and challenges are analysed in Chapter 4 to develop a roadmap for responsible use of AI-powered video surveillance in Chapter 5.

Chapter 3: Research Design and Methodology

This chapter details the research design and methodology that is followed throughout this work. First, the relevance of the choice of topic and research objectives are explained: the definition of AI-powered video surveillance and how it works helps to better understand the debate between proponents and opponents and justify the relevance of the topic.

Second, the selection of the case studies is explained, with the analysis divided into two case studies, object-centred AI-powered video surveillance and person-centred AI-powered video surveillance.

Once the selection of case studies is justified, the data collection and the different steps that constitute the data analysis are explained. This research relies on Document Analysis and coding to make sense of the information found in the collected data. However, the starting point of the analysis is anchored in securitisation theory to better understand the polarisation of the debate on the use of AI-powered video surveillance. This lays the foundations to go beyond the frames imposed by each side of the debate to understand the real capabilities of the technology.

Document Analysis is then used to collect and analyse the data, in combination with the coding of the qualitative data. Two types of data sources and documents are used – policy documents and technical documents – to confront different perspectives. Document Analysis and coding together allow extracting the opportunities and challenges of each application of AI-powered video surveillance to give a comprehensive overview.

Relevance of choice of topic and research objectives

This dissertation aims to provide a roadmap for responsible use of AI-powered video surveillance for predictive policing by law enforcement. AI-powered video surveillance refers to the use of AI in video surveillance, with the

recognition of visual data – objects, humans, emotions, events, etc. This technology was popularised by the proliferation of surveillance cameras and the emergence of video analytics (VA), the processing of videos with algorithms to complete security-related tasks (Norman, 2017; Olatunji and Cheng, 2019). AI-powered video surveillance is an application of video analytics, the "automatic processing and understanding of video content in order to determine or detect spatio-temporal events and extract information or knowledge about the observed scene" (Olatunji and Cheng, 2019, p.3). Its development comes from a desire to fight crime through video surveillance more efficiently by automating the analysis of videos and fully exploiting the vast amount of data produced by cameras (Olatunji and Cheng, 2019). It constantly incorporates newly developed techniques and algorithms, combining cameras with different data sources such as social media, and has several application areas, from healthcare to transport or security (Olatunji and Cheng, 2019). In security, it is applied to biometrics, detection and tracking, and behaviour analysis, among others. Video is segmented into millions of frames and sets of still images (Olatunji and Cheng, 2019). Many images are needed to feed the algorithms and allow AI systems to analyse what a given entity looks like (IPVM, 2022). At the most basic level, the algorithm detects an object, then, whether the object is a person or not, finally categorises it as either person, vehicle, animal or inanimate object (IPVM, 2022). Beyond entity detection, there are some more complex applications which include behaviour detection of people but also of objects, for instance intrusion, people counting, and objects left behind or removed (IPVM, 2022).

However, the use of this technology has led to a polarised debate around the world, including in the EU, on whether to ban it, particularly in the case of person-centred video surveillance. Data protection and privacy advocates have drawn attention to several ethical issues related to the risk of false alerts, errors and misclassifications (IPVM, 2022). The large amount of data required to run the algorithms is of concern as it promotes increased harvesting of personal data

and the proliferation of mass surveillance, as well as a potential infringement of the right to privacy. These challenges can lead to many other human rights violations, such as increased discrimination.

Yet the technology offers significant opportunities to better fight crime, which by extension would also have a positive impact on human rights by saving lives. Rather than investigating a cost-benefit ratio in terms of security vs. freedom, this dissertation argues for the need to understand the real capabilities of technology, avoiding technological sensationalism. The choice to study the challenges and opportunities of AI-powered video surveillance therefore stems from the observation that EU institutions struggle to grasp the real capabilities of the technology, which should however be the guiding principle of any regulatory development. The author aims to provide a better understanding of some of the applications of AI in video surveillance to offer a roadmap for a responsible use for more appropriate regulation that considers a realistic approach to the possibilities supported by the technology. As such, the research objectives are summarised as follows:

1. Build and analyse a database of existing policies and technical documents on AI-powered video surveillance
2. Synthesise challenges and opportunities of AI-powered video surveillance
3. Provide a roadmap for responsible use of AI-powered video surveillance to EU policymakers.

Selection and definition of the case studies

This dissertation focuses on how AI-powered video surveillance for predictive policing by law enforcement can be responsibly implemented in the EU. To do this, it relies on a selection of specific documents that allow to determine opportunities and challenges, to establish a roadmap for responsible use of AI-

powered video surveillance. The analysis is divided into two parts, hereafter referred to as case studies, corresponding to two different types of applications of AI-powered video surveillance used for visual recognition: object-centred AI-powered video surveillance and person-centred AI-powered video surveillance.

- *Object-centred AI-powered video surveillance* refers to AI-powered video surveillance that focuses on objects, with applications such as object recognition or detection of object intrusion into a scene.
- *Person-centred AI-powered video surveillance* refers to AI-powered video surveillance focused on individuals, with for example facial recognition technologies, crowd monitoring or violence detection.

The choice to structure applications into two distinct groups is explained by the fact that each variety of topic of interest brings its own opportunities and challenges, although there are sometimes overlaps. For example, the stakes for AI-powered video surveillance focused on people are much higher than those focused on objects. Indeed, surveillance technologies are much more intrusive and problematic for individuals' privacy rights than for objects, which are more impersonal and whose surveillance therefore seems more justifiable. Therefore, these opportunities and challenges need to be considered to develop a proportionate and effective regulation.

Starting from securitisation theory

The first step of the analysis is to briefly situate the public debate surrounding the given application. Using securitisation theory, previously defined in the literature review as a process whereby actors transform ordinary political issues into security issues to legitimate the use of extraordinary measures in the name of security, the analysis of each case study begins by giving an account of how each side of the debate frames the use of the AI-powered video surveillance.

This account does not constitute the core of the analysis of this research and is not concerned with collecting data to analyse discourse. Rather, the use of securitisation theory corresponds to a contextualisation effort which must be understood as the starting point of the analysis. Hence, it lays the basis to go beyond such frames in the analysis, where qualitative data is collected and analysed to understand the actual opportunities and challenges of the AI applications and establish a roadmap for a responsible use of the technology.

Towards collecting the qualitative data

The second step of this dissertation is to build a database that gathers different documents that will constitute the qualitative data that will then be analysed using Document Analysis and coding of the qualitative data.

As the field of AI-powered video surveillance is relatively new, the author includes sources from different countries to offer a variety of approaches. Ultimately, this dissertation aims to inform regulatory action in the EU on the responsible use of AI-powered video surveillance by understanding the challenges and opportunities. Thus, while the roadmap for responsible use is intended for EU policymakers, the case studies are enriched by lessons learned in other countries, if applicable to EU concerns.

The types of documents collected are grouped into two different types. These correspond to different types of data sources, which allow the author to triangulate the results to identify the opportunities and challenges of AI applications while taking the most objective approach possible. This choice is made to have a nuanced and balanced approach between policy choices, realistic observations of what the different applications can do and a better understanding of their implications. The two types of documents are defined as follows:

- *Policy documents*:

Policy documents firstly consist of existing regulations and legislations from the EU itself, but also from within the Member States and relevant third countries, originating from governmental and institutional sources. They also include policy briefs and governance recommendations from relevant independent regulatory bodies, parliamentarian groups or think tanks.

- *Technical documents:*

Technical documents firstly consist of press releases and websites of private entities developing and selling AI-powered video surveillance solutions. The internal workings of the technologies being confidential and protected by their proprietary nature pose limitations to understanding the actual performance of the solutions. To go beyond the marketing communication aspect of the latter documents, which tends to overestimate the capabilities, technical academic articles are also included, offering a more objective view of the technologies' capabilities.

This research is limited in terms of accessibility of literature due to the language limitation of the author. The research is therefore mainly based on primary sources available in French and English, as well as secondary sources to gather insights from other regions. Further limitations specific to the applications are specified in the 'Presenting the data' section of each case.

Analysing the data through Document Analysis and Coding

Once the data is selected, the author proceeds to the analysis of the collected qualitative data through Document Analysis. The author assigns codes to categorise the data and conducts inductive reasoning that goes from the specific to generalisations to establish key opportunities and challenges of each branch of application determined. The same steps are followed for each of the case studies.

Document Analysis is "a systematic procedure for reviewing or evaluating documents" (Bowen, 2009, p.27). Document analysis procedure includes "finding, selecting, appraising (making sense of), and synthesising data contained in documents" and "yields data […] that are then organised into major themes, categories, and case examples specifically through content analysis" (Bowen, 2009, p.28).

Document Analysis is particularly applicable to qualitative case studies, although some limitations can be found such as a potential selection bias (Bowen, 2009). According to Bowen (2009), such selection bias can be overcome through triangulation. The latter refers to "a method used to increase the credibility and validity of research findings" (Noble and Heale, 2019). For instance, conducting interviews is a method that can be used to complement Document Analysis (Bowen, 2009). Still, Document Analysis can also be used as a stand-alone method (Bowen, 2009). It is the case in this research, which is based on analysing documents by extracting opportunities and challenges of the technology. However, to increase reliability, this research uses different data sources. This allows for a triangulation that gives a complete understanding of the phenomenon of AI-powered video surveillance, seeking convergence, and corroboration but also finding gaps between the different sources.

The author then adopts an inductive approach by reading and assigning codes throughout the research to reach general conclusions about the opportunities and challenges offered by each branch of application. Coding plays an important role in the analysis of qualitative data as it allows for the categorisation and to sort the information found in the documents. Codes can be simple words, sentences or paragraphs (Basit, 2003). They help to make sense of the documents by finding commonalities, differences and patterns that allow the researcher to make generalisations about a phenomenon and understand the situation as a whole (Basit, 2003). The established list of codes for each branch of application can be found in the 'Presenting the data' sections of each case.

Finally, this analysis helps to establish a roadmap for responsible use of AI-powered video surveillance, provided in the first part of the discussion in Chapter 5. The second part of Chapter 5 also goes beyond the technology itself and questions the wider system in which AI-powered video surveillance is embedded and serves. It argues that responsible use of AI-powered video surveillance can only really be achieved if wider policing practices are challenged.

Chapter 4: Analysis

The case analysed focuses on object-centred AI-powered video surveillance, while the second one focuses on person-centred AI-powered video surveillance.

Object-centred AI-powered video surveillance

Object-centred AI-powered video surveillance refers to AI-powered video surveillance that focuses on objects, with applications such as object recognition or detection of object intrusion into and across a scene. First, the selected data used for the analysis is presented, acknowledging its limitations. Second, the issue of securitisation is tackled as a starting point for the analysis. Third, the opportunities of the technology are established from the database, starting with its technical capabilities, and followed by its positive implications for the better protection of citizens. Fourth, the challenges of the technology are established from the database, starting with its technical limitations, and followed by its negative implications for human rights. Finally, a roadmap for responsible use of the technology is provided.

Presenting the data

The database encompasses 42 documents in total which can be found in Appendix I. These were divided into two main categories: 1) technical documents; 2) policy documents. Each of these categories was divided into two sub-categories:

- Technical documents:
    - Solutions offered by businesses to predict and prevent crime: websites of companies, white papers produced by companies,

but also news articles testifying on a given solution when the latter was not available anymore: 14 documents
    - Technical academic papers to verify capabilities: 9 documents
- Policy documents:
    - Existing legislations and regulations in the EU and beyond that can be leveraged and applied to the technology: 9 documents
    - Reports with considerations and recommendations on the use of the technology from independent bodies (regulatory and independent bodies, parliamentary discussion groups, think tanks): 10 documents

The inductive reasoning allowed to go from specific observations to general conclusions to analyse the key opportunities and challenges of the technology. The generated codes are classified into four different categories and several sub-codes. The codes can be found in the following table:

Table 1: Codes taken from the collected and analysed data on object-centred AI-powered video surveillance

Code category	**Sub-codes and key information found and analysed in the database**
Technical capabilities	• Available algorithms: CNN, R-CNN, Fast and Faster R-CNN, YOLO v1-5 • Available datasets: COCO • Available applications and techniques: object detection; object tracking, object classification
Technical limitations	• Processing power, accuracy and speed • Limited datasets • Variability: size, shape, occlusion, deformation, viewpoints variations, lighting conditions, background subtractions,

Positive implications	• Crime prediction and prevention solutions, kinds of crimes covered: dangerous objects, unattended objects, stolen objects, suspicious objects • Support to law enforcement: efficiency, cost, reallocation of resources • Improvement of human rights: prediction and prevention of crime, opportunities for privacy
Negative implications	• Threats/implications for human rights: normalisation of mass surveillance, increased mistrust in population, data protection and privacy threats, accountability issues, technological solutionism

Several limitations must be considered. Firstly, the legislation and regulations governing the use of this technology are currently limited to those governing traditional video surveillance of public space. Independent bodies are beginning to address the opportunities and challenges posed by the technology to encourage legislators to update regulations to consider the risk posed by object surveillance too. Ultimately, concerns about the technology are related to human rights, as object-centred AI-powered video surveillance involves extensive surveillance of public spaces where people also appear, and objects can reveal information about people, providing a back channel for the leakage of potentially sensitive data about individuals. Finally, business solutions tended to largely oversell their products, a challenge which was mitigated using academic technical paper to understand its real capabilities.

Securitising object-centred AI-powered video surveillance

Object-centred AI-powered video surveillance is not *per se* at the forefront of the general debate on the use of AI video surveillance. It is a much less hot topic

than person-centred AI-powered video surveillance, for obvious reasons: it involves objects, which are not people, and are therefore not subject to the same scrutiny regarding ethical issues such as data protection and privacy.

Proponents of the technology securitise the threat environment, advocating object recognition to detect suspicious and dangerous objects commonly used in crime such as guns or knives, to better prevent street crime. This research found that private security actors providing the technology play a very active role in securitising the threat environment to incite law enforcement but also private individuals to use their systems. This research finds that their marketing strategies put forward crime rates, violent crimes such as terrorism or mass shootings, but also non-violent crimes such as theft or incivility, and highlight the lack of resources of law enforcement agencies. Other securitising actors include governmental and law enforcement authorities.

In contrast, critics securitise the tool, automated smart cameras, pointing to the risk of invasion of privacy as these cameras are widely deployed in public spaces. For them, automated smart cameras promote mass surveillance and threaten human rights. Securitising actors include data rights and privacy advocates, and more broadly human rights NGOs.

In the end, the securitisation of object-centred AI-powered video surveillance is very much linked to people: on the one hand, governments and law enforcement claim their desire to use all possible means to better protect populations, supported by private companies who securitise the threat environment to market their product, while critics legitimately warn against privacy threats.

The debate on the development of smart cities is a good example object-centred AI-powered application that sparks the securitisation of video surveillance. Smart cities are urban centres that harness a network of sensors that collect real-time information from multiple interconnected devices to improve city management and service delivery (Feldstein, 2019). Multiple automated smart cameras used for object-centred AI-powered video surveillance are installed all over cities to allow law enforcement to access a

continuous stream of information to better predict and manage crime in real-time. Proponents see an opportunity to improve crime prevention, build safer cities and maximise resources through remote surveillance, while critics warn against normalising and promoting mass surveillance under the guise of improving the lives of citizens.

Object-centred AI-powered video surveillance offers opportunities to better fight crime but also raises legitimate concerns, which are tackled in the following sections.

Exploring opportunities and challenges of object-centred AI-powered video surveillance

Opportunities

This section first focuses on the technical capabilities of object-centred AI-powered video surveillance found in the database to understand what the technology can do. Then, it looks at its positive implications, including protecting citizens, saving resources, and potentially improving privacy.

Technical capabilities

Object-centred AI-powered video surveillance usually uses Deep Learning (DL) for machines to recognise, classify visual data and learn from experience. DL is a type of ML that mimics the way humans acquire knowledge. Several DL models are used for visual recognition, the most popular and performant being region-based models and single-shot detector models (Jha et al., 2021). The choice of model depends on what needs to be achieved, and there is often a trade-off between speed and accuracy (Deci, 2021). For instance, within region-based models, Convolutional Neural Networks (CNN) are particularly efficient to detect, distinguish and classify objects. They are frequently used due to their robust structure, processing performance, and ability to reduce classification errors (Araujo et al., 2020; Jang et, al. 2020). Other kinds of DL algorithms include single-shot detectors such as You Only Look Once (YOLO) algorithms,

popular due to their speed (Jang et al., 2020). Therefore, algorithms used to monitor objects largely depend on the objective sought and allow to build solutions adapted to the needs. Beyond algorithms, high-quality cameras and high-performance computers are required to process the large quantity of visual data needed to feed the algorithms (Fundee et al., 2019; Abdulghafoor and Abdullah, 2022).

Object-centred AI-powered video surveillance includes several applications, prominent ones being object detection and tracking. Generally, algorithms are firstly trained to detect whether a given object is present within a frame in real-time, to recognise which object it is and where it is in the image, and eventually, to track it across frames, throughout the sequence of images that constitute videos (Idrees and Shah, 2017; Fundee et al., 2019).

Object detection is achieved by training classifiers, which assign labels to a set of images allowing programs to recognise objects by mathematically differentiating them (Indrees and Shah, 2017). Humans select relevant features from videos to label, a process known as the extraction of a bounding box, to build a collection of images that algorithms learn to recognise that will be classified into these pre-defined categories during deployment (Porikli and Yilmaz, 2012; Indrees and Shah, 2017; Araujo et al., 2020). Multiple datasets are available to train models, such as the COCO dataset provided by Microsoft which includes a collection of over 300,000 images and 80 object categories (Saikia et al., 2017).

Object tracking is done in different ways, by tracking the area where the moving object is located, or by tracking the contours or certain characteristics of the object (Zhang and Klette, 2003). Algorithms detect changes in the pixelation state of an image between video frames, a process called ‘change detection’. It uses different techniques too, such as ‘frame differentiation’, which recognises the differences between two successive frames through a change in pixelation that implies that the image is changing; ‘background subtraction’, which consists of constructing a representation of the background and detecting

deviations from this representation; or ‘motion segmentation’, which assigns different classes to groups of pixels based on the speed and direction of their movements (Porikli and Yilmaz, 2012).

Positive implications

This next section looks at the positive implications of the technology gathered in the database. First, object-centred AI-powered video surveillance allows to better protect citizens through the detection and tracking of suspicious, dangerous and stolen objects. Then, the technology allows for saving resources. Finally, it has promising applications for improving privacy while monitoring public spaces.

Protecting citizens through object detection and tracking to predict and prevent crime

Algorithms can recognise suspicious objects, such as unattended luggage, dangerous objects, such as weapons, or stolen objects, such as cars (Jang et al., 2022). The definition of what qualifies as suspicious is decided by the solution designers: for example, Jang et al. (2022) built their models on public data from the Korean government’s crime statistics to classify the objects most frequently used to commit a crime as dangerous. The solutions gathered in the database and analysed do not disclose their algorithms due to their property nature, but their capabilities matched what was gathered in the technical academic literature, although they often oversold their speed and accuracy. The detection of suspicious objects was the most common application found in the analysed data for object-centred AI-powered video surveillance, allowing to send alerts to law enforcement when flagging dangerous objects, with weapon detection and tracking being most prominent. None of the solutions analysed claimed to replace law enforcement, but rather to support them by taking charge of the first step in the response chain, namely alerting. BriefCam, for example, says to provide a quick review and real-time alert of suspicious objects to law enforcement, who then assess the threat and act (BriefCam, n.d.). Other widespread applications for suspicious objects found in the data include the

detection of unattended objects and the detection and tracking of stolen objects to prevent thefts in real-time. Finally, Automatic Licence Plate Recognition (ALPR) links the collection of number plates with law enforcement databases to recognise car owners and track their movements. In the context of predictive policing, ALPRs are used in cases of traffic incivilities, escapes from crime scenes or attempted kidnappings.

Saving resources

The data analysed argues that object-centred AI-powered video surveillance reduces the workload of law enforcement officers. It is an effective technology that allows to automate police work and reallocate resources so that officers can focus on other essential tasks. Automated smart cameras are more efficient and provide continuous surveillance. They are not prone to fatigue and detect even small objects at a distance which are difficult for the human eye to see, while the proliferation of cameras has made it impossible for a human to review all the visual data collected. Additionally, the rarity of abnormal events does not justify losing officers to this task.

The technology is therefore cost-effective, with the solutions collected in the database showing that software can simply be implemented on existing camera networks rather than requiring the purchase of new smart cameras (La Vigne et al., 2011). Moreover, such cameras can be purchased by private individuals and connected to law enforcement databases, thus increasing the coverage of monitored cameras at a lower cost (Ng, 2020).

Improving privacy

This of course raises questions of accountability, data protection and privacy since ultimately, object surveillance requires the surveillance of public spaces where individuals are present and whose personal data must be protected. This research did not find any regulation that specifically regulates the use of object-centred AI-powered video surveillance, probably due to its focus on objects rather than people preventing it from being a ‘high risk’ use of AI-powered

video surveillance. The *Commission Nationale de l'Informatique et des Libertés* (CNIL), the French independent privacy regulator, however, points out the need for new regulations on intelligent smart cameras (2022). Existing regulations can also be used to prevent overburdening the use of the technology. This research finds that many legislations regulate the broader use of video surveillance, with indications such as stating the purpose of and justifying the need for video surveillance, placing a video surveillance warning sign, or determining limited data retention periods. An additional advantage of automated smart cameras is their ability to blur irrelevant entities, encrypt visual data and record and report only detected suspicious objects to agents, which ultimately offers possibilities to improve privacy as it prevents constant recording and watching by humans. The object recognition solution Keymakr for instance offers to secure data through encryption, data expiration and the use of VPNs (Nomerovska, 2021).

Challenges

This section first focuses on the technical limitations of object-centred AI-powered video surveillance found in the database to understand what the technology cannot do. Then, it looks at its negative implications, including overlooking data protection and privacy issues, accountability and the risk of normalisation of mass surveillance and technological solutionism.

Technical limitations

The first set of limitations of object-centred AI-powered video surveillance stems from the datasets used to train the algorithms. The qualitative data analysed shows that solution designers face difficulties in training the algorithms because visual recognition algorithms require a large amount of visual data to operate, which is more difficult to collect than other types of data. For example, data protection and privacy issues may hinder the collection of visual data. In addition, visual data is not always of high quality depending on the camera model, and its processing requires a lot of computing power (Jha et

al., 2021). High-quality material is costly and can put a strain on law enforcement resources. The processing of visual data is even more complex when the technology is deployed in non-benign and unpredictable environments, as the algorithms will be confronted with some objects that they have never learned to recognise or track (Porikli and Yilmaz, 2012). This has implications for accuracy but also for the speed of detection and tracking, causing law enforcement agencies to lose valuable time in detecting potential future crimes.

Beyond data collection and datasets issues, object-centred AI-powered video surveillance faces the problem of image variability: object detection and tracking algorithms need to generalise to important object variations such as occlusion, changes in lighting conditions and viewpoints or image quality (Porikli and Yilmaz, 2012). First, occlusion occurs when several objects come closer together in an image, with DL algorithms mistakenly identifying as one new object (Zhang and Klette, 2003; Meel, n.d.). This phenomenon is common as images contain numerous fast-moving visual data (Porikli and Yilmaz, 2012). The object of interest can quickly be masked by other objects, making detection, identification and tracking difficult. Occlusion can be partial or total, with partial occlusion being particularly difficult for DL algorithms to spot due to the new shape of objects that are missing some parts and features (Porikli and Yilmaz, 2012). As such, variations in viewpoints, deformation of objects, and even the variety of size, shape and colour of an object can render the task difficult (Porikli and Yilmaz, 2012).

Additionally, background distractions can also occur. Backgrounds can be cluttered or textured, making object detection and tracking difficult (Meel, n.d.). Unfortunately, in non-benign environments, backgrounds are rarely monochrome (Meel, n.d.). This can lead to object recognition errors, especially when searching for small objects. Furthermore, changes in lighting conditions also make object detection and tracking difficult, as lighting has a significant impact on the definition of objects, which can look very different depending on

light exposure (Araujo et al., 2020). Moreover, rapidly changing video environments require algorithms to be trained to perform rapid analysis to detect, classify and track relevant objects accurately (Idrees and Shah, 2017). Algorithms therefore need to be trained to maintain their performance when faced with uncertainties, which means making them more robust to changes in distribution and adversaries. Errors can be made deliberately: object-centred AI video surveillance can be deliberately confused, avoided or even neutralised by adversaries. This brings the issue of surveillance avoidance back to the question of whether it is worth deploying technology that could be easily rendered ineffective.

All these factors have an impact on the accuracy of the prediction and can lead to errors. These errors have real-life consequences as they prevent law enforcement agencies from fulfilling their mission. They must be considered, proving that law enforcement cannot just rely on technology and that they must always be included in the decision loop to prevent or mitigate potential algorithmic errors.

Negative implications

Negative implications of object-centred AI-powered video surveillance stem from the deployment of the technology on a large scale in public spaces and are ultimately connected to human rights issues.

Overlooking data protection and privacy issues

As mentioned, existing regulations and legislations analysed in the database do not cover object-centred AI-powered video surveillance, as automated smart cameras do not fall under specific regulations. However, regulatory bodies such as the French CNIL (2022) are calling on governments to legislate on the changing nature of cameras, arguing that automated data processing completely changes the nature and scope of video surveillance. Spaces are no longer simply filmed but analysed, which is not an evolution of traditional cameras but rather a profound change in their operating systems.

It is also difficult to determine which objects can be considered sensitive. ALPRs, for example, should be considered sensitive data because they are linked to the personal information of a human being. However, the scope of the analysed legislation in automated video surveillance is generally limited to biometric data, neglecting objects that may provide sensitive information about humans by extension. Existing European directives for instance are not sufficient since they only focus on data explicitly linked to persons such as biometrics.

Moreover, this technology is versatile as the parameters can be easily changed from monitoring objects to monitoring people (CNIL, 2022). However, the data used for this analysis shows that the safeguards are not sufficient to prevent or monitor such a change. It is therefore necessary to set up verification and control bodies to ensure that the expected parameters are respected, not only to ensure that law enforcement agencies but also private companies providing the technology do not abuse their power.

Accountability

The object-centred AI-powered video surveillance solutions analysed in the database were provided by private companies. This is not a problem in itself: computers or firearms are not designed and produced by law enforcement officers who use them. However, these products are regulated by safeguards: for example, firearms must answer to certain norms and officers need a licence to use them. This research found that such safeguards are lacking for object-centred AI-powered video surveillance solutions. The auditing of algorithms proves to be difficult not only due to their proprietary nature but also due to their complexity, as their designers themselves do not always understand how ML algorithms work (Leese, 2020). Even if they had access to them, supervisory bodies would therefore not necessarily be able to understand how the algorithms work, hence the need to find alternative means of accountability, for example by introducing mandatory result evaluations and impact assessments.

The normalisation of mass surveillance and risk of technological solutionism

Object-centred AI-powered video surveillance requires a large amount of visual data, which requires the deployment of a vast network of cameras. This further normalises insidious and generalised mass surveillance of public spaces, which can increase citizens' distrust and self-censorship. Furthermore, authorities must be careful not to fall into the trap of technological solutionism often promoted by smart cities, which claims that automated smart cameras will predict and prevent all crimes. The deployment of object-centred AI-powered video surveillance must be proportionate and justified. Furthermore, the use of this technology itself is not an answer to crime, it is simply a tool that can help to better predict it. A recurring example identified through this research is the use of gun detection to better prevent mass shootings in the US. While it is intended to save lives, the real issue to be addressed here is gun control. The use of technology will not neutralise the root causes of mass shootings in the country, but rather apply a band-aid solution until the next tragedy. Other solutions should therefore be considered to reduce crime rates in cities and provide a sustainable and effective response to crime.

Person-centred AI-powered video surveillance

Person-centred AI-powered video surveillance refers to AI-powered video surveillance focused on individuals, with for example facial recognition technologies, crowd monitoring or violence detection. First, the selected data used for the analysis is presented, acknowledging its limitations. Second, the issue of securitisation is tackled as a starting point for the analysis. Third, the opportunities of the technology are established from the database, including its technical capabilities, and its positive implications for the better protection of citizens. Fourth, the challenges of the technology are established from the database, starting with its technical limitations, and followed by its negative implications for human rights.

Presenting the data

The database encompasses 57 documents in total which can be found in Appendix II. These were divided into two main categories: 1) technical documents; 2) policy documents. Each of these categories was divided into two sub-categories:

- Technical documents:
    - Solutions proposed by companies and reports on solutions implemented by governments or law enforcement agencies: 9 documents
    - Technical academic papers to verify capabilities: 22documents
- Policy documents:
    - Existing legislations and regulations in the EU and beyond that can be leveraged and applied to the technology: 14 documents. Due to language barriers, some academic documents were also used to understand legislative frameworks in other countries.

- Reports with considerations and recommendations on the use of the technology from independent bodies (regulatory bodies, parliamentary discussion groups, think tanks): 12 documents

The inductive reasoning allowed to go from specific observations to general conclusions to analyse the key opportunities and challenges of the technology. The generated codes are classified into four different categories and several sub-codes. The codes can be found in the following table:

Table 2: Codes taken from the collected and analysed data on person-centred AI-powered video surveillance

Code category	**Sub-codes and key information found and analysed in the database**
Technical capabilities	• Available databases: open source; proprietary (companies); criminal/non-criminal (law enforcement) • Available processing: real-time; post-event/crime • Available applications: person detection; face detection; abnormal behaviour and movement detection; facial recognition
Technical limitations	• Challenges in training datasets: lack of data available; lack of diversity • Challenges in data captured: changing conditions; occlusion; mismatch between training/testing and deployment
Positive implications	• Crime prediction and prevention solutions: spotting confirmed criminal behaviours; spotting the possibility of future crime • Specific kinds of crimes covered: abnormal and violent behaviours; identification, tracking and

	apprehending of suspected and confirmed criminals • Improvement of human rights: mitigation of surveillance
Negative implications	• Threats to privacy including data protection and interoperability issues • Consequences of threat to privacy: threat to freedom of association, assembly and expression; power imbalance; mistrust and fear of mass surveillance • Bias in design; in training datasets; classification; data collection; processing (algorithmic bias) • Consequences of bias: discrimination; stigmatisation; errors

A few points should be considered. There was more data available for person-centred than for object-centred AI-powered video surveillance. In the laws and regulations analysed, regulatory efforts in person-centred AI-powered video surveillance fall under data protection and privacy laws as they concern the management of personal data considered sensitive. Regulatory efforts governing the use of AI specifically are still in their early stages, with the EU offering the most comprehensive regulatory text, the AI Act (2021), which is yet to be adopted. Much of the commercial solutions found for person-centred AI-powered video surveillance were not only destined for law enforcement purposes but also for market analytics, company premises and private individual home security. The overwhelming majority of person-centred AI-powered video surveillance concerned facial recognition.

Securitising person-centred AI-powered video surveillance

Person-centred AI-powered video surveillance crystallises the debate around the use of AI-powered video surveillance, for the obvious reason that it directly involves people. Facial recognition features prominently, and more specifically live facial recognition.

This research finds that proponents of the technology put forward its ability to keep cities and people safe, finding an unprecedented opportunity to improve crime prevention. They also advocate for its use in analysing post-crime scenes and conducting investigations, applications which go beyond the scope of this dissertation. In this case, the securitised object is the threat environment: the use of the technology is being justified by increasing crime rates and incivilities in cities. The inability of law enforcement to tackle such threats due to strained resources is also put forward to justify the use of the technology that offers a cost-efficient response. Securitising actors are found in governmental authorities, on local, regional, and national levels alike.

Meanwhile, critics are very worried about the effects of the use of technology on human rights. They fear widespread mass surveillance and chilling effects on individuals that would threaten fundamental rights such as freedom of association, the right to privacy or the presumption of innocence, among others. Thus, the securitised object is the tool itself as it poses risks to individual freedoms. Securitising actors in this case are found in human rights NGOs, data protection and privacy activists and advocacy groups, or political parties.

The use of facial recognition applications is the most striking example of securitisation of the technology and polarisation of the debate. Proponents advocate its use to better protect citizens while opponents fear its impacts on fundamental rights. As such, proponents either actively promote the use of the technology or support its use under certain conditions, with safeguards (Ragazzi et al., 2021). In contrast, some opponents argue for a precautionary principle,

advocating for a moratorium on the use of the technology for the time being, to better identify the many unknown risks at present (Ragazzi et al., 2021). Other opponents advocate for an outright ban on the technology, deeming it completely incompatible with democratic values (Ragazzi et al., 2021).

Finally, this research found that private companies may have played a less prominent role in securitising the threat environment to call for the use of the technology than in the case of object-centred AI-powered video surveillance. On the contrary, some companies have actually participated in securitising the tool, or more specifically law enforcement's behaviour and their use of the tool, to justify stopping the development of their solutions. IBM, Microsoft, and Amazon, themselves have recently introduced a moratorium, restricted the use or stopped producing person-centred AI-powered video surveillance technologies (BBC, 2020a; BBC, 2020b; Hill, 2022). For instance, Amazon imposed a moratorium on the use of its facial recognition software Rekognition by law enforcement in the US following the murder of George Floyd, an African-American, by a police officer (BBC, 2020b).

Person-centred AI-powered video surveillance offers opportunities to better fight crime but also raises legitimate concerns, which are tackled in the following sections.

Exploring the challenges and opportunities of person-centred AI-powered video surveillance

Opportunities

This section focuses on the technical capabilities of person-centred AI-powered video surveillance found in the database to understand what the technology can do. Then, it looks at its positive implications, including identifying, tracking and apprehending suspected and confirmed criminals alike to prevent crime, as well as mitigating the impact of surveillance.

Technical capabilities

At a basic level, person-centred AI-powered video surveillance works like object-centred AI-powered video surveillance. With person detection, the camera evaluates the presence of a person in an image: people are processed as a type of 'object', with the camera classifying the entity as 'person'. Similarly, face detection specifically detects human faces and assesses the presence and position of individuals in the image (Ragazzi et al., 2021).

At a more complex level, person-centred AI-powered video surveillance analyses human action and recognises specific human behaviours. It assumes that identifiable patterns of behaviour precede the perpetration of criminal activity. The identification and detection of these signs would therefore allow knowing that a crime is about to be committed and to act accordingly to prevent it (Podoletz, 2022). The technology typically works in two steps (Mabrouk and Zagrouba, 2018). It firstly detects the region of interest in which the person is moving and extracts relevant features. Then, it processes human actions to provide information about human behaviour. For abnormal behaviour detection, the technology assesses whether the action is 'normal'. The algorithm is trained to recognise certain behaviours as 'normal': what does not follow this baseline is therefore considered 'abnormal' and triggers an alert warning (Kim et al., 2021). More complex algorithms classify behaviour under more specific types of actions, for example violence detection (Deniz et al., 2014). This kind of application requires to be fast and accurate to spot rapid actions, strong processing power, and large training datasets (Sreenu and Durai, 2018). The latter comes from a variety of sources, and the classification of actions as 'abnormal', 'violent' or other, depends greatly on the designers (Accattoli et al., 2020).

For facial recognition, algorithms build on face detection and recognise who is in the video image by comparing the collected visual data to a database to find a match. These databases are made up of pictures collected by law

enforcement or governments, for example from mugshots in criminal records but also from more controversial sources (Ragazzi et al., 2021). The technology can also extract relevant features and classify them into specific categories, such as ‘old’ or ‘woman’ (Black et al., 2021).

Facial recognition also allows the user to follow and track the target through different frames. In this case, the algorithm confirms that the same individual appears in different frames rather than looking for a match (Ragazzi et al., 2021).

Progressing from facial recognition, emotion recognition can also be conducted to understand the emotional state of people using their facial cues and body language to either understand existing criminal behaviour or the possibility of future crime (Black et al., 2021; Podoletz, 2022) However, emotion recognition is rare and its efficiency remains to be proven (Ragazzi et al., 2021; Podoletz, 2022).

Finally, person-centred AI-powered video surveillance can be carried out in real-time or not, both applications being suitable for predictive policing purposes. Live surveillance allows real-time alerts to be sent to identify suspicious behaviour and track targets while delayed surveillance allows to identify crime patterns, prevent offences and recidivism (Ragazzi et al., 2021). The technology is therefore broadly classified into two branches of application: the first one identifies confirmed criminal behaviour, while the second one identifies behavioural indicators that could point to the potential of future crime (Podoletz, 2022). Understanding these differences is important because they bring about different implications that should be considered in regulation.

Positive implications

This section examines the positive implications of the technology collected in the database. Since the argument of cost-efficiency tackled for object-centred AI-powered video surveillance applies here too, this section leaves out this opportunity. It first explores how the technology can help identify, track, and

apprehend suspected and confirmed criminals to prevent crime. It then explains how the technology can help mitigate the impact of surveillance.

Identifying, tracking, and apprehending suspected and confirmed criminals to predict and prevent crime

Person-centred AI-powered video surveillance can help apprehend suspected and confirmed criminals, prevent offences and recidivism, assuming that a criminal is likely to re-offend, and thus break patterns of crime.

Person-centred AI-powered video surveillance, specifically face detection and facial recognition technologies, can help law enforcement agencies to authenticate, verify the identity of or identify suspected or confirmed criminals. Facial recognition, for example, can be used to search or monitor targeted individuals, enabling law enforcement to track and apprehend suspected and confirmed criminals alike (UK Parliamentary Office of Science and Technology, 2002). For example, the York Area Regional Police Department identified and located a man who had groomed online and sexually assaulted a teenager, finding a match after several months of cross-referencing his photo with its database through facial recognition (Schuetz, 2021). This arrest not only brought the man to justice but may also have prevented him from committing another crime, which ends up being an opportunity for breaking patterns of crime.

Besides, person-centred AI video surveillance can help victims of crime as it can identify and locate victims of human trafficking or missing children, for example, allowing law enforcement to better support vulnerable and at-risk individuals (Leslie, 2020; Information Commissioner's Opinion, 2021).

Furthermore, the technology can spot behaviours indicating that crime may occur, thereby allowing law enforcement to act and prevent escalation. The technology monitors public areas to spot incidents and better coordinate law enforcement's action. It can detect abnormal behaviours, such as incivilities, trespassing, loitering, falls and violence, to make cities safer (Kim et al., 2021). The prediction and identification of specific movements are particularly useful

in emergencies since it allows one to quickly spot a dangerous situation and notify law enforcement on time (ICO, 2021). Person detection, for example, can identify individuals who should not be on particular premises, while facial recognition could determine whether these individuals regularly return to the location, which could help identify stalkers or potential thieves.

Violence detection provides another good example. The detection of violent actions can prevent the spread of mass violence by enabling law enforcement to act before human lives or properties are threatened (Halder and Chatterjee, 2020). It can also help law enforcement assess how dangerous a situation is and be better prepared to ensure their own safety and that of potential victims when arriving on the scene. Additionally, violence detection technologies could be used to monitor law enforcement itself and prevent police brutality and abuse, increasing officers' accountability (Abo Software, n.d.).

Mitigating the impact of surveillance

Remote monitoring is often considered nonobtrusive by its advocates. Indeed, it may be considered less intrusive than police patrolling and randomly searching individuals across cities. It can also be optimised to be less intrusive. First, cameras can be programmed to record scenes only when events are reported. The faces of non-targeted people can be automatically blurred or hidden. Additionally, the collected data can be effectively protected through the automatic encryption of stored data and authentication methods to access the data (Casteel et al., 2006).

Further steps may be found to render the technology less invasive. The development of X-ray machines at airports provides an example of good practice: originally, privacy advocates opposed them since they could give a view of the whole human body. However, technology evolved so that most revealing techniques were no longer used, although there is still room for improvement (Berti, 2020). Ultimately, this method allows not to be touched directly by the agents, guaranteeing the safety of people while limiting the feeling of intrusion. Solutions for adapting person-centred AI-powered video

surveillance could also be developed to ensure safety and comfort, allowing for remote surveillance that is less invasive than other kinds of biometrics such as DNA or fingerprints (Mann and Smith, 2017).

Moreover, the collected literature suggests that the development of clear procedures for law enforcement to follow when using the technology strengthens safeguards and helps improve privacy by design. This includes a clear statement of purpose, data minimisation, the determination of a retention and access period for the data, and encryption of visual data.

Challenges

This section first focuses on the technical limitations of person-centred AI-powered video surveillance found in the database to understand what the technology cannot do. Then, it looks at its negative implications, including impacts on privacy and related rights and issues of bias and discrimination.

Technical limitations

Technical limitations firstly emerge with the training datasets themselves. Person-centred AI-powered video surveillance requires large training datasets to adequately train the algorithm. The collection of such image databases is difficult, albeit legitimately, due to the sensitive nature of biometrics. Additionally, training data must be diverse for algorithms to be properly trained and tested so that they are accurate, robust, and adaptable when deployed in the real world. If requirements for accuracy and robustness are not met, risks of errors when deployed increase, which have dramatic consequences for individuals.

Furthermore, technical limitations emerge from the data captured by the cameras themselves. Datasets are trained for specific purposes which do not necessarily correspond to real-life use, a mismatch that leads to errors (Ragazzi et al., 2021). Moreover, the training environment is much different from the real-life one where algorithms face numerous changing conditions. These include changes in lighting, physical characteristics of individuals that differ

from the training dataset but also change appearance throughout the video, putting on or taking off objects (glasses, hat, beard, etc.) (Mabrouk and Zagrouba, 2018; Ragazzi et al., 2021). Image resolution decreases greatly with these changing conditions, and the ability of cameras to monitor an area efficiently also greatly depends on the orientation and the area covered by the cameras. The latter is easily occluded in crowded scenes (Ragazzi et al., 2021). Occlusion can be voluntary or not: many opponents to person-centred AI video surveillance do not want to be monitored and deliberately confuse the algorithms. During the recent protests in Hong Kong, for example, protesters altered or masked their facial features to avoid facial recognition (Mahtani and Hassan, 2019).

Most solutions found in the literature, whether academic or commercial, claim high-efficiency scores when testing their algorithms. However, testing takes place under optimal and controlled conditions that do not reflect real-world conditions (Ragazzi et al., 2021). Testing is therefore not sufficient and needs to be accompanied by frequent evaluation and impact assessment to effectively assess the efficiency of algorithms. This is currently not being done sufficiently, and guidelines for doing so are sorely lacking, as the data analysed in this research shows. If efficiency is not properly assessed, the risk of error will remain high, which in the case of person-centred AI video surveillance has important human rights implications.

Negative implications for human rights

This section looks at the negative implications of the technology for human rights, as gathered in the database. It focuses on the most salient issues to offer a deep understanding of the stakes, starting with the impacts on privacy and related rights and followed by issues of bias and discrimination.

Impacts on privacy and related rights

Person-centred AI-powered video surveillance demonstrates obvious risks for data protection and privacy rights. Data shows that it captures massive amounts

of personal data, some of which are very sensitive personal data, such as biometrics, but also associated sensitive data which can for instance map individuals' habits (EDPB, 2020). Hence it poses heightened risks to data subjects' rights, threatening privacy and anonymity (GDPR, 2016). Additionally, the technology threatens the right to informational self-determination[2], consent and individuals' control of their personal data (Podoletz, 2022).

Beyond the obvious invasion of privacy related to the monitoring of public spaces, there are also concerns with law enforcement databases themselves. Reported cases show that law enforcement criminal databases such as mugshots have been mixed up with non-criminal databases such as driving license pictures (Turner Lee and Chin, 2022). The interoperability of these databases is an issue for privacy because non-criminals do not consent to have their pictures processed for criminal purposes and may not even beware of such developments. Additionally, reports show that law enforcement in the US has purchased data from data brokers or gained access from first-party service providers (Turner Lee and Chin, 2022). This practice threatens data subjects because there is a lack of consent, awareness and accountability among law enforcement and companies alike.

Person-centred AI-powered video surveillance threatens privacy through the normalisation of mass and continuous surveillance. This research reveals a lack of awareness among citizens of the operation and implications of the technology, whether it is the changing nature of video surveillance from simply monitoring people to analysing them or the versatility of the technology and its implications for human rights (CNIL, 2022). It creates a power imbalance, with public agencies and private companies developing software retaining critical information to the public (Garvie et al., 2016). Citizens are not

[2] Power of an individual to decide for him/herself when and to what extent information about his/her private life may be communicated to third parties (Rouvroy and Poullet, 2009).

involved in the discussion while such an important change in the nature of surveillance should be subject to deliberation, allowing individuals to be aware, consulted and seek approval before implementing such technology (CNIL, 2022; Garvie et al., 2016). Individuals may not agree to such increased surveillance, feeling uncomfortable with being monitored continuously to the point of changing their behaviours because they fear behaving in a way that would be considered 'abnormal' (GDPR, 2016). This lack of privacy could put pressure on citizens, deter them and hinder their rights to freedom of movement, assembly or association, or freedom of expression, with a negative effect on democratic values and participation (Casteel et al., 2006; Leslie, 2020).

The use of biometric collection tools in public spaces should therefore be accompanied by strict safeguards and procedures for law enforcement. This research finds that these are currently sorely lacking in the EU and elsewhere. Other types of biometrics, such as the collection of fingerprints for which a warrant is required, already benefit from strict and specific measures. Regarding person-centred AI-powered video surveillance, the policies reviewed in this analysis focus largely on *when not to use* the technology, but rarely on *how to use it* when authorised. Yet this is where regulation has the most important role to play, and where the EU could use its normative power to promote its democratic values to ensure that the information collected serves a defined purpose and avoid any misuse (Mann and Smith, 2017).

Bias and discrimination

Bias in person-centred AI video surveillance is complex and longstanding. The collection of visual data itself is linked to historical racism, with nineteenth-century cameras able to capture light skins far better than black skins (Podoletz, 2022). These biases in the design of cameras and visual data collection persist today and have even been reinforced by algorithms. New forms of discrimination have emerged due to biased sampling practices, data collection and labelling, datasets and data pre-processing and modelling (Podoletz, 2022).

Algorithms also carry normative choices: the purpose and way in which they are developed, as well as the data that feed them, are based on the operational choices, motivations, and intentions of the designers (CNIL, 2022).

Bias already exists in the training stage of the algorithms. Training datasets lack diversity, which prevents algorithms from accurately detecting and classifying certain demographics, thus reinforcing societal biases (Buolawmini and Gebru, 2018). Numerous studies show that facial recognition algorithms are much less effective on darker-skinned women, leading to differential treatment, errors and abuse such as wrongful arrests (Buolawmini and Gebru, 2018; Grother et al., 2019). Existing algorithms tend to perpetuate confirmation bias: the outcome predicted by the algorithm reinforces the biases, unconscious or not, that were used to produce it (Ragazzi et al., 2021).

Furthermore, the very idea of categorising humans by inventing classifications for their physical characteristics and behaviours is fraught with bias and builds on long-standing practices of mapping and profiling that are tainted by racism, sexism, and ableism (Mann and Smith, 2017; Wendehorst and Duller, 2021). The labelling of data is greatly subjective and lacks accuracy which leads to algorithmic discrimination. Indeed, classifications are often binary and fail to consider the nuance of the real world, unable to accurately reflect markers such as age, gender, or ethnicity (Ragazzi et al., 2021). Classification relies heavily on stereotypes and assumptions about people, which leads to risks of inappropriate inferences, stigmatisation, and discrimination (Wenderhost and Duller, 2021). This is particularly tangible in abnormal behaviour detection since what is deemed and classified abnormal in one situation or context may not be in another, with algorithms lacking the ability to contextualise.

Thus, instead of correcting human biases, algorithms reinforce them leading to ever greater disparities and mistreatment. This can have dramatic consequences for individuals, with heightened discrimination such as the wrongful arrest of

innocent people. Minorities, marginalised and vulnerable people are particularly at risk of being misidentified for a crime with which they have not committed since algorithms are more likely to misclassify and produce errors with them (Turner Lee and Chin, 2022).

Chapter 5: Discussion

This discussion chapter first presents the roadmap for responsible use of AI-powered video surveillance, derived from the analysis. AI-powered video surveillance is considered a single practice that enables different applications, either object-centred or person-centred, each of which in turn has many other applications. Therefore, the five main considerations for responsible use are:

- The nature of the collected visual data, purpose and alternative options
- Technical limitations and how to overcome them
- Leveraging and reviewing existing regulatory frameworks
- Developing clear safeguards and procedures for use
- Keeping humans in the loop.

The second part of this discussion chapter argues that the responsible implementation of AI-powered video surveillance requires challenging the system in which the technology is embedded and which it serves. It questions current practices of crime prevention and predictive policing, highlights the role of securitisation in legitimising these practices and addresses the issue of surveillance avoidance. Overall, it proposes to go beyond the technology itself and challenge the current crime prevention system to move the debate on the use of AI-powered video surveillance forward.

A roadmap for responsible use of AI-powered video surveillance

Considering the nature of the collected visual data, purpose, and alternative options

The first consideration for the responsible use of AI-powering video surveillance is the importance of considering the different types of applications of the technology. This includes taking into account the sensitivity of the visual

data being collected, the purpose and reason for the surveillance, as well as other potentially better-suited solutions.

Beyond the monitored entity, person or object, the degree of sensitivity of the collected data should be considered. This research shows that object monitoring could be a backchannel to providing sensitive information about people, as is the case of ALPR. In the meantime, crowd monitoring, which is not aimed a specific people but can be used for instance for counting people in a given space, is not as intrusive and does not collect sensitive data since it does not provide specific information about people. What qualifies data as sensitive must be reassessed, considering the changing nature of video surveillance. The fact that cameras no longer only monitor areas but also analyse them presents increased risks. Data that was previously not seen as sensitive can become so because of the ability of algorithms to aggregate data and make sense of it to give information about people, regardless of the nature of the target entity – object or people.

Furthermore, the type of automated surveillance is also to consider. AI-powered video surveillance was classified into two types: a first one that identifies justified suspected and confirmed criminal behaviour, and a second one that identifies behavioural indicators that could point to the potential of future crime (Podoletz, 2022). This difference is fundamental. In the first case, law enforcement *knows* that a crime has been committed or has *sufficient grounds* for pursuing an investigation. It is therefore legally and ethically justified into taking actions such as monitoring suspected and confirmed criminals to apprehend individuals and prevent them from re-offending, or to apprehend the victims to better support them. AI-powered video surveillance also has an evidence collection and forensic role to play too, but this goes beyond the scope of this research.

The second case is more problematic from an ethical and legal point of view because there is no real basis to justify the surveillance: it is not known

that a crime is going to be committed, nor who is being sought and for what reasons. It is general surveillance of a place to try to find clues that a crime might be committed. This practice highlights the contemporary desire to manage the unease and is fully representative of the 'risk society' obsessed with the notion of prevention and control of risk (Beck, 1986).

Finally, when talking about purposes, alternative options should also be considered. Technology supports law enforcement to predict and prevent crime but cannot address the root causes of crime. Policymakers must be careful not to rely on technology to lower crime rates and fix issues that are endemic to society and requires a much more comprehensive response which considers the socio-economic factors of crime. Impact assessment can be useful to assess what solution is better fitted to prevent crime and whether AI-powered video surveillance is necessary or if alternative solutions are better suited.

Overcoming technical limitations

The responsible use of AI-powered video surveillance also includes increasing the quality of the technology's performance. Governments have a duty to ensure that technical challenges are overcome to ensure the safety, accuracy, and reliability of the technology by introducing relevant standards and supporting innovation to achieve such requirements. This section discusses the main technical issues that need to be resolved before deploying the technology.

The first problem concerns the training datasets. Training algorithms require large and diverse datasets. Particular care should be taken to ensure that the algorithms are fed with diverse data for proper training and testing. This would increase ML robustness and confidence in predictions and avoid errors, false positives, and false negatives.

However, it is not enough to have algorithms that perform well in a training environment: they also need to perform well when deployed in the real world, in non-benign environments. This requires frequent evaluation and

impact assessment to ensure the accuracy of ML models and that the algorithms perform as they are intended to.

Finally, concerns could be addressed by improving the technology and incorporating security at the design stage, promoting 'security by design'. For example, much of the debate about AI-powered video surveillance stems from privacy concerns. This research has shown that some technologies could be improved and modified to address these concerns, for example by only recording when an abnormal event is reported, by blurring 'irrelevant' entities, or by directly encrypting and protecting the visual data collected.

Leveraging and reviewing existing regulatory frameworks

Another important consideration for responsible use is to build on and review existing regulatory frameworks. This would avoid regulatory overload that could hamper innovation.

This research firstly reveals that globally, AI-powered video surveillance is primarily regulated by data protection and privacy laws. In the US, there are currently no federal data protection and privacy laws for public and commercial use alike. The Fourth Amendment of the Constitution does however guarantee the right of people to be secure against unreasonable searches and seizures, which can be used to prevent abuse of video surveillance. Furthermore, some state and local governments have introduced data protection and privacy regulatory schemes to regulate the public sector, and some cities such as San Francisco have decided to ban facial recognition (Conger et al., 2019). The UK further benefits from a Surveillance Camera Code of Practice which is currently going under revisions to guide the appropriate use of surveillance cameras by law enforcement and local authorities. Even China has just enacted its first Personal Information Protection Law (PIPL) (Luo and Gup, 2021). Although it contains an article to regulate facial recognition, is still too fragile to adequately regulate the use of AI-powered video surveillance and

leaves the door open to many cases of abuse against targeted minorities such as the Uyghurs (Luo and Gup, 2021).

Meanwhile, the European Union has opted for a uniform framework that offers the most extensive data protection and privacy laws with the introduction of the General Data Protection Regulation (GDPR, 2016). Additionally, the Law Enforcement Directive (LED, 2016) provides further guidance for the processing of criminal data to prevent, investigate, detect, and prosecute criminal offences. These two regulatory texts currently govern the rights of data subjects and law enforcement's obligations in terms of video surveillance.

More broadly, this research also shows that AI regulation is underway globally, regulation which could also govern the use of AI-powered video surveillance. The EU is developing the most advanced piece of regulation, the AI Act, which promotes a risk-based approach to differentiate 'unacceptable' risks from 'high' and 'low to minimum' risks. The AI Act would prohibit the 'most harmful AI systems' which create 'unacceptable risks' while laying down mandatory requirements for 'high risk' AI systems, hence allowing for more freedom for 'low to minimal risk' systems and promoting an innovation-friendly framework. However, the AI Act has many shortcomings, including unclear definitions of what is considered 'harmful', of the definition of AI itself, as well as unclear guidelines for conformity assessments of high-risk systems, leaving providers to self-assess under certain conditions. Additionally, the obligations of users of AI systems are also unclear, while those of developers are simply lacking.

Therefore, this research shows that there are applicable, but not necessarily comprehensive, frameworks for regulating the use of AI-powered video surveillance. These can serve as a basis for regulation but need to be reassessed given the changing nature of video surveillance and the re-evaluation of what makes the data sensitive. Finally, it would be useful to provide guidelines on

how to use the technology when it is allowed, rather than focusing the regulation on *when* it can be used or not.

Developing clear safeguards and procedures for use

Subsequently, policymakers must now focus on establishing clear rules, with safeguards and procedures, for when and how to use the technology. If these requirements are not met, the technology should simply not be used. It will require a massive effort to understand all the issues, combining a realistic approach to the applications that can actually be implemented with a good understanding of its human rights implications, to establish appropriate thresholds.

These safeguards and procedures should be put in place for use by law enforcement, to offer data subjects guidelines to retrieve their data, and for private companies developing AI-powered video surveillance solutions, especially if these are intended for use by public actors. Based on the findings of this research, the following sections highlight key considerations for the development of such safeguards and procedures.

Firstly, measures must already be taken to decide on the deployment of the technology. This should be subject to public consultation and a cost-benefit analysis including human rights impact assessments.

Second, clear procedures must be established for the use of the technology by law enforcement, which includes a stated purpose, data minimisation, restricted data access, appropriate data retention and evaluation. The stated purpose of the surveillance must be legitimate and proportionate and set out clear limitations to understand the conditions under which the surveillance is permitted. For example, surveillance could only be allowed in cases of serious threats or reasonable suspicion of a crime (Casteel et al., 2006). Moreover, law enforcement authorities must meet data minimisation requirements so that only the data necessary for the stated purpose are collected.

Additionally, data access rules with strict limitations must be guaranteed by a clear legal basis and involve supervisory authorities. Certain measures can be taken to restrict access to data: for example, law enforcement authorities could be required to provide a warrant to access certain visual data from public surveillance systems, as they would to collect any other type of sensitive data such as DNA (Schuetz, 2021).

Moreover, visual data must be stored appropriately: safeguards can be implemented, such as end-to-end protection or visual data encryption. Law enforcement databases should also be kept up to date and law enforcement agencies should ensure that criminal data is not mixed with non-criminal data.

Finally, evaluation and impact assessment procedures are important safeguards to implement. These could be carried out externally under the supervision of an independent supervisory authority. The evaluation and impact assessment should also be reviewed frequently to ensure that potential impacts on fundamental rights are still properly addressed. They should be conducted to ensure data protection, accuracy and effectiveness of the systems.

Thirdly, data protection procedures for data subjects must also be clearly established to respect people's data and privacy rights. Individuals must always be informed that a given area is under surveillance by a warning sign, and be given additional information about the data collected, purpose, retention period and access on another platform, for example online. This is already provided for in most of the video-surveillance regulations analysed in this research. For their part, law enforcement authorities must respond to individuals who request access to their data. Finally, potential abuses should be regulated by safeguards and remedies should be available in case of harm and abuse.

Finally, clear guidelines should be established for developers, solution providers and system integrators. Policymakers should encourage standardisation and certification and provide licences for the sale of technology. A fundamental change in the technology of a solution should thus be subject to re-licensing.

Developers and suppliers need to ensure the quality and accuracy of data and algorithms to be compliant and to guarantee security and privacy by design. Additional measures must also be taken to prohibit the sharing of data with third parties and to ensure that data access is respected. Finally, regarding the problems of bias and unfairness posed by algorithms, discriminatory practices should be clearly identified and prohibited. Solutions that do not meet the requirements of accuracy and robustness should simply not be put on the market. Frequent evaluation of the performance and accuracy of the systems could help take out such solutions from the market.

Keeping (all) humans in the loop

Finally, humans must always be kept in the loop. This firstly means keeping law enforcement in the loop. Whatever the application of AI-powered video surveillance, the technology should always be used to support law enforcement, not replace it. It should be seen as a tool for law enforcement to do their job. Under no circumstances should officers rely solely on the predictions of technology to make decisions. AI-powered video surveillance is there to complete the first step in the response chain by flagging abnormal events and sending alerts. Law enforcement must then make informed decisions, using their own training, experience, and critical analysis to assess a situation and take appropriate action. Finally, they should also be provided with the necessary training to ensure the good functioning of the technology.

Furthermore, citizens must be included in the process of deployment of AI-powered video surveillance. This research shows that this is not the case anywhere in the world, except when civil society organisations unite to challenge policymakers and demand more regulation. This is a problem regardless of what technology can or cannot do. Citizens are the first to be affected by this technology, whether increased surveillance brings greater security or harms their privacy. They should therefore have a say in this debate.

After 9/11 and the subsequent war on terror, American citizens expected their government to take all necessary measures to better protect themselves (Romaniuk and Webb, 2015). The US government abused this trust. Citizens did not feel comfortable with the government monitoring their communications as it was. The outcry over Edward Snowden's revelations in 2013 shows that the public cares about what governments exactly do to protect citizens (Lyon, 2015; Tréguer, 2017). This is also the case in Europe, where the affair caused a stir (Lyon, 2015). Citizens expect to be protected, but they also expect to be at least a minimum informed about what is being done to achieve that goal (Lyon, 2015). There should be a broader open conversation with citizens about the implications of data-driven surveillance.

Fears and concerns about this technology are legitimate and should be acknowledged. AI-powered video surveillance is a technical subject that is not necessarily accessible to a non-technical audience. Providing citizens with the information and tools to understand what is being discussed is an essential first step in a democracy, before implementing a system that has far-reaching implications.

Thus, awareness-raising campaigns should also be organised to inform and involve citizens so that they can make an informed choice about the model of society in which they wish to live. The changing nature and generalised use of AI-powered video surveillance should then be subject to public consultation and deliberation, and citizens' approval should be sought. This would help decrease the power imbalance between governing bodies and citizens, ensuring greater transparency in the process, and is a necessary step in reducing public distrust of law enforcement and government.

Going beyond the technology to challenge the system

This section goes beyond the technology to question the role of the system in which AI-powered video surveillance is embedded in the responsible

implementation of the technology. Firstly, it links the findings to the literature review by questioning current crime prevention practices and predictive policing. Second, it highlights the role of securitisation in legitimising these practices and proposes to shift the debate from the technology itself to the broader crime prevention system. Finally, it addresses the issue of surveillance avoidance to reiterate the importance of public consultation, which is sorely lacking in the current system.

The roadmap has highlighted the main considerations that need to be taken into account by policymakers to enable the responsible use of AI-powered video surveillance. The findings of this research show that it is not currently possible to implement all AI-powered video surveillance applications responsibly, but that some crucial steps can be taken to move in this direction. The technology has an undeniable ability to better predict and prevent crime, but not all applications have yet reached the same levels of maturity required for responsible use. In addition, some applications have far-reaching implications for human rights that need to be considered.

However, understanding the opportunities and challenges to determine what improvements can be made to promote better practice in the use of technology is not enough to know how to deploy it responsibly. One must also consider the system that the technology will serve. Writer William Gibson (1995) states in an interview that "technologies are morally neutral until we apply them. It's only when we use them for good or evil that they become good or evil". This suggests that a tool is just a tool and that it is the users' intended purposes that make the tool good or bad. Technology is therefore not neutral as its use can have positive or negative implications depending on the purpose. Therefore, technology cannot and should not be expected to correct the problems of the system in which it is developed and implemented, as it actually reflects and serves that system. The ML models used for AI-powered video surveillance provide a tangible example of these expectations, as the algorithms were

originally intended to be able to correct human bias by providing neutral processing of the data. However, research shows that this is not the case: on the contrary, ML models reproduce and even reinforce the biases leading to erroneous predictions, due to the biases already present in the datasets and the training of the algorithms.

Beyond these far-reaching technical limitations, the mere idea of preventing a crime that has not yet been committed seems problematic in a punitive pre-emption system. While technology could be used to improve crime prevention by addressing its root causes, it is instead used to focus on crime deterrence. Current law enforcement practices in crime prevention focus more on understanding *how* crimes are committed than *why* they are committed, which does not allow for the development of long-term solutions that would reduce crime by addressing its root causes. However, this issue goes beyond law enforcement: it is a broader policy issue. Indeed, crime prevention relies on law enforcement and their policing strategies and tactics to counter threats in a preventive manner, rather than integrating other crime prevention actors such as social workers or communities (Sherman et al., 1998). If law enforcement, and governments, must prevent crime wherever possible, they can choose how to do it, and how to use algorithmic predictions to develop a more sustainable response to crime. The debate about the use of AI-powered video surveillance, or any other law enforcement tool for that matter, should perhaps focus more on challenging the wider policing system and practices rather than the technology itself.

To do so means challenging the current perspective on crime prevention. The latter is currently largely based on the notion of pre-crime, the idea that law enforcement should aim to reduce and eliminate crime, rather than reacting to and investigating crimes after they have occurred (Asaro, 2019; Egbert and Leese, 2020). Predictive policing is seen as a means of achieving this goal, using large amounts of data and pattern recognition to identify at-risk situations,

people or places. It makes estimates about the future and allows law enforcement to act based on an assessment of the risk and likelihood of the crime occurring (Egbert and Leese, 2020). AI-powered video surveillance is one of the tools that enable this type of policing, using visual data to determine crime patterns and allow law enforcement to react before the crime is committed. ML has enabled cameras to become a tool for predictive policing, as previously cameras were only a passive technology whose main interest was to analyse crime scenes (Lindsey and Woolf, 2021). This further shows that the current practice of AI-powered video surveillance, whether object-based or person-based, is embedded in a particular type of crime prevention system based on predictive policing and the processing of large amounts of data through pattern recognition to predict crime.

Securitisation plays an important role in legitimising these practices. It makes it possible to establish an issue as a security issue that requires exceptional measures to protect citizens (Romaniuk and Webb, 2015). This process is therefore a political choice that illustrates a desire to counter a threat, whether real or not, through the enactment of exceptional measures. In the case of AI-powered video surveillance, this research shows that the technology was subjected to a twofold securitisation process. First, government authorities and law enforcement agencies have been engaging in that process. They securitise the threat environment to legitimise the use of the technology, highlighting their desire to better protect citizens and reduce crime rates. They are largely supported by private security actors who have commercial interests in promoting the technology. These different actors therefore highlight the opportunities of the technology to justify its ability to fight crime. Conversely, the challenges posed by the technology provide fertile ground for critics to argue against its use. Data protection and privacy advocates securitise the technology itself to justify the need for introducing a moratorium or banning the technology altogether. To move forward in this particularly polarised debate, it is necessary to understand both sides of the issue, step back from the noise and understand

what the real opportunities and challenges of the technology are. It also means looking beyond the technology itself, since it is neither good, bad nor neutral, and questioning the wider policing system into which the technology is embedded and which it serves.

Finally, the usefulness of the technology must be questioned as the problem of surveillance avoidance remains. Even if policymakers were to regulate the technology responsibly, adversaries could still decide to fool the algorithms used for AI-powered video surveillance, preventing it from working. What then is the point of implementing the technology if it can still be fooled? This question remains to be explored further in the academic literature. From a purely technical point of view, this means improving the robustness of the technology to defeat adversaries. Politically, it means convincing opponents not to fool the technology. There is only one way to do this in a democracy: to bring the issue to consultation and foster a healthy debate that considers those directly affected by the policies. Developing technology that is understood, negotiated, and accepted by individuals is the best way to avoid adversaries.

Chapter 6: Conclusion

This dissertation investigates how AI-powered video surveillance for predictive policing purposes could be responsibly implemented, if at all. The initial assumption of the research was that responsible use could be achieved if the real opportunities and challenges of the technology were better understood and considered to develop an appropriate and proportionate regulatory approach. A ban on the technology was not seen as a viable option, as it prevents the possibility of innovation and improvement of the technology to match EU values. On the contrary, a ban can lead the EU to lose its normative power to other powers that continue to develop and deploy AI-powered video surveillance globally and do not share the same human rights standards. The findings confirm the initial assumption and further argue to challenge the wider crime prevention and predictive policing practices in which the technology is embedded and which it serves, to ensure responsible use, as summarised in the next paragraphs.

The debate around the use of AI-powered video surveillance is highly polarised in the EU. Each actor in the debate is engaged in a securitisation process. On the one hand, the proponents of the technology, governments, law enforcement and private security actors, securitise the threat environment, crime in cities, to justify the introduction of exceptional measures, the use of AI-powered video surveillance, to counter the threat. On the other hand, opponents of the technology, data rights and privacy advocates, securitise AI-powered video surveillance itself, to justify exceptional measures, in this case a moratorium or ban on the technology. This debate, rooted in rhetoric, influences the different regulatory approaches to the use of AI-powered video surveillance. This research moves away from this polarised debate, as the academic space allows for a more nuanced approach to the issue. It argues that the implementation of AI-powered video surveillance firstly requires a

comprehensive understanding of the technology, considering what it can and cannot do. Determining the technical capabilities and limitations provides an understanding of the positive and negative implications of the technology which should form the basis of any regulatory approach.

The first step in this direction is to consider the type of entity being monitored, which has a significant impact on decision-making. Targeting an object has very different implications than monitoring a person, due to the sensitive nature of personal data. Therefore, the analysis was divided into two parts: object-centred and person-centred AI-powered video surveillance. Within each of these branches, several applications were considered. Object-centred AI-powered video surveillance included object detection and tracking, while person-centred AI-powered video surveillance included person and face detection, abnormal behaviour detection, and facial and emotion recognition. Understanding that AI-powered video surveillance encompasses many different types of applications is essential for the development of proportionate regulation. These applications also do not meet the same level of maturity, efficiency, and accuracy. This gives rise to different implications that need to be considered for an appropriate regulatory framework.

Through document and content analysis of policy and technical documents, this research establishes the opportunities and challenges for object-centred and person-centred AI-powered video surveillance to develop a roadmap for the responsible use of the technology. The findings show many similarities in terms of technical capabilities and limitations, as well as positive and negative implications.

Regarding technical capabilities, findings show that both branches of application detect, recognise, and classify a given entity. This is the first step toward any kind of visual recognition application. Additionally, applications can further offer the ability to track items across frames. The monitored entities depend on what the algorithms have been trained to recognise. Entities range

from a broad category of people (suspected or confirmed criminals, victims, etc), objects (knife, gun, blood, etc) and behaviours (violent actions, kicking, falling, etc) associated with crime.

Similar technical limitations were also found in both cases. They firstly stem from the training datasets in the training phase since AI-powered video surveillance requires a large amount of visual data, which must be diverse and classified accurately. The research shows that training datasets often lack this diversity and that classifications are not always accurate which leads to prediction errors. Additionally, there is a mismatch between the training and testing environment in which the technology is developed and the real-world environment in which the technology is deployed. AI-powered video surveillance relies on ML algorithms which are trained in benign and predictable environments. When deployed in the real world, they encounter many adversaries and changing conditions which challenge algorithms and lead to prediction errors. Such changing conditions are particularly tangible in video surveillance, with visual data being subject to a rapidly changing environment due to changes in lighting, background noises, or occlusion.

These technical capabilities and limitations have far-reaching implications. There is again a lot of overlap between object-centred and person-centred AI-powered video surveillance. These implications, even if the entity monitored is an object, all have to do with impacts on humans.

The positive implications fully converge. Both object-centred and person-centred AI-powered video surveillance allow for better protection of citizens through identification and tracking. Moreover, both make a cost-effective argument, as the technology supports law enforcement in the time-consuming and human error-prone practice of video surveillance. Finally, the technology could even have a positive impact on improving the privacy of video surveillance and mitigating surveillance practices if it is adapted to current concerns.

The negative implications differ a little, as person-centred AI-powered video surveillance deals with particularly sensitive data and its impacts on citizens are much more direct. However, the findings show that object surveillance can be a back channel to reveal sensitive information about individuals too. Therefore, the first negative implication noted in each case is the threat to the privacy and data of individuals. In addition, AI-powered video surveillance as a whole presents risks of normalising mass surveillance with related threats to freedom of association, assembly and expression due to the continuous monitoring of public spaces. Moreover, there is also a tendency toward technological solutionism, with the idea that technology can solve all crime issues, at the expense of alternative solutions that are better suited to fighting crime in the long term. Furthermore, prediction errors can make law enforcement waste valuable time in the fight against crime, and lead to the unjustified arrest of innocent people. In particular, person-centred AI surveillance remains extremely prone to biases that lead to discrimination. Finally, accountability issues also arise due to the lack of transparency and safeguards surrounding the use of this technology.

As a result, the responsible use of AI-powered video surveillance requires several considerations which are set out in the roadmap. The latter includes considering the nature of the collected visual data, purpose and alternative options; overcoming technical limitations; leveraging and reviewing existing regulatory frameworks; developing clear safeguards and procedures for use and evaluation; and keeping humans in the loop. These are all necessary to guarantee a clear framework which ensures protecting the rights of citizens, guaranteeing transparency and accountability while allowing for innovation to support law enforcement and improve crime prevention techniques.

Beyond the technology itself, this research finds that the responsible use of the technology cannot be achieved without considering the system in which it is developed and which it serves. A tool is merely a tool, and what makes it

good or bad is the use that is made of it. The current crime prevention system is largely based on the notion of pre-crime with the idea that law enforcement should aim at reducing and even eliminating crime, instead of reacting and investigating crimes after they occur, using deterrence and punitive policing practices. This prevents the development of alternative and sustainable solutions to crime that address its root causes. It also links back to the risk of technical solutionism, the belief that technology can solve any issues at the expense of long-term socio-economic policies. Therefore, the debate and regulatory attempts should go beyond the technology itself and challenge the current crime prevention system to achieve responsible use of AI-powered video surveillance.

Nevertheless, the findings of this research confirm the initial assumption that a total ban on the technology is not the right approach to regulating the use of AI-enabled video surveillance in the EU. The diversity of applications of AI video surveillance does not justify a complete and outright ban. This research shows that measures can, and should, be put in place to improve each of these applications and guarantee responsible use. A ban on the technology would prevent the EU from taking advantage of the opportunities offered by the different applications to fight crime. It would also prevent the EU from fully understanding the negative implications of this technology, and from finding ways for adaptation to make it more responsible.

Meanwhile, other powers that have not banned this technology will continue to develop it by setting their own standards that may not fit EU democratic principles. The EU would then lose its normative power and its ability to set standards that reflect its values. The GDPR has demonstrated the EU's potential to set high standards of data protection and privacy that have been copied around the world: this shows that its normative power exists and that it could and should be harnessed in the case of AI-powered video surveillance. The forthcoming AI Act is an important step in the development of the responsible use of AI-powered video surveillance and could have a similar normative impact to the

GDPR if it considers the real opportunities and challenges of AI, its multiple uses, and its positive and negative implications.

Bibliography

Abdulghafoor, N. H., and Abdullah, H. N. (2022) A novel real-time multiple objects detection and tracking framework for different challenges. *Alexandra Engineering Journal*. 61 (12), pp. 9637-9647.

Abo Software. (2018) *Violence Detection for Smart Surveillance Systems*. Available from: https://www.abtosoftware.com/blog/violence-detection [Accessed 24 July 2022].

Accattoli, S., Sernani, P., Falcionelli, N., Mekuria, D. N., and Dragoni, A. F. (2020) Violence Detection in Videos by Combining 3D Convolutional Neural Networks and Support Vector Machines. *Applied Artificial Intelligence*. 34 (4), pp. 329-344.

AccessNow. (2018). *Human Rights in the Age of Artificial Intelligence*, pp. 1-40. Available from: https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf [Accessed 24 July 2022].

Amodei, D, Olah, C, Steinhardt, J, Christiano, P, Schulman, J, and Mané, D. (2016). Concrete Problems in AI Safety. 1-29. Available from: https://arxiv.org/pdf/1606.06565.pdf [Accessed 24 July 2022]

Araújo, P., Fontinele, J. and Oliveira, L. (2020) Multi-Perspective Object Detection for remote Criminal Analysis Using Drones. *IEEE Geoscience and Remote Sensing Letters*. 17 (7), pp. 1283-12816.

Ariel, B. (2019) Technology in Policing. In: Weisburd, D and Braga, A. (eds.) *Police innovation: Contrasting perspectives*. Cambridge, UK, Cambridge University Press, pp. 483-563.

Asaro, P. M. (2019) AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care. *IEEE Technology and Society Magazine*. 38 (2), pp. 40-53.

Balzacq, T. (2005) The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations*. 11 (2), pp. 171-201.

Barocca, J G. (2021) Surveillance and Predictive Policing Through AI Urban Future with a Purpose. In: Deloitte, *Urban Trends: Shaping the future of Cities*. Available from: https://www2.deloitte.com/global/en/pages/public-sector/articles/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html [Accessed 24 July 2022].

Basit, T. (2003) Manual or electronic? The role of coding in qualitative data analysis. *Educational Research*. 45 (2), pp. 143-154.

BBC. (2020a) IBM abandons 'biased' facial recognition tech. *BBC*, 9 June. Available from: https://www.bbc.com/news/technology-52978191 [Accessed 24 July 2022].

BBC. (2020b) George Floyd: Amazon bans police use of facial recognition tech. *BBC, 11 June.* Available from: https://www.bbc.com/news/business-52989128 [Accessed 24 July 2022].

Beck, U. (1986) *Risk society: towards a new modernity*. London Etc.: Sage.

Berti, A. (2020) Timeline: The history of airport body scanners. *Airport Technology*, 6 April. Available from: https://www.airport-technology.com/analysis/history-of-body-scanners/ [Accessed 24 July 2022].

Bertuzzi, L. (2021) Europol nears stronger mandata for data-driven policing capacities. *Euractiv*, 12 October. Available from: https://www.euractiv.com/section/justice-home-affairs/news/europol-nears-stronger-mandate-for-data-driven-policing-capacities/ [Accessed 24 July 2022].

Bigo, D. (2020) Covid-19 tracking apps, or: how to deal with a pandemic most unsuccessfully. *about:intel*. Available from: https://aboutintel.eu/covid-digital-tracking/ [Accessed 24 July 2022].

Black, D. (2021) Facial analysis: automated surveillance and the attempt to quantify emotion. *Information, Communication and Society*, pp. 1-14.

Bourbeau, P. (2015) Securitization. *International Encyclopedia of the Social and Behavioral Sciences*. 2nd ed, pp. 395-399.

Bowen, G. (2009) Document analysis as a qualitative research method. *Qualitative Research Journal*. 9 (2), pp. 27-40.

Briefcam (n.d.). *Search & Review Hours of Video in Minutes*. BriefCam. Available from: https://www.briefcam.com/solutions/review-search/ [Accessed 24 Jul. 2022].

Browning, M. and Arrigo, B. (2020) Stop and Risk: Policing, Data, and the Digital Age of Discrimination. *American Journal of Criminal Justice*. 46, pp. 298-316.

Buil-Gil, D., Moretti, A. and Langton, S. H. (2021) The Accuracy of Crime Statistics: Assessing the Impact of Police Data Bias on Geographic Crime Analysis. *Journal of Experimental Criminology*, pp. 1-28.

Buolawmini, J. and Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*. 81, pp. 1-15.

Busuioc, M. (2020) Accountable Artificial Intelligence: Holding Algorithms to Account. *Public Administration Review*. 8 (5), pp. 825-836.

Buzan, B;, Waever, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*. Boulder, Lynne Rienner Publishers.

Casteel, E., Monroe, K.A., Ribeiro, P.G., Warren, R.A., Bradford Franklin, S., Onek, J.N. and Sloan, V.E. (2006). *Guidelines for Public Video Surveillance: A guide to protecting communities and preserving liberties*. Washington DC: The Constitution Project, pp. 1-60. Available from: https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf [Accessed 24 July 2022].

CNIL (2022). *Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics position sur les conditions de déploiement*, pp. 1-18. Available from: https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf [Accessed 24 July 2022].

Conger, K., Fausset, R. and Kovaleski, S.F. (2019). San Francisco Bans Facial Recognition Technology. *The New York Times*, 14 May. Available from: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [Accessed 24 July 2022].

Couchman, H. (2019). *Policing by Machine: Predictive Policing and the Threat to our Rights*, pp. 1-48. Available: https://www.libertyhumanrights.org.uk/issue/policing-by-machine/. [Accessed 24 July 2022].

Crawford, A. and Evans, K. (2012) Crime Prevention and Community Safety. In: Maguire, M., Morgen, R., and Reiner, R. (eds.) *The Oxford Handbook of Criminology*. Oxford, UK, Oxford University Press, pp. 769–805.

Deci (2021) The Object Detection Landscape: Accuracy vs Runtime. *Deci*, 24 May. Available from: https://deci.ai/blog/object-detection-landscape-accuracy-vs-runtime/. [Accessed 24 July 2022].

Delbecque, E. (2015) *Idéologie Sécuritaire et Société de Surveillance : le Storytelling du XXIe Siècle*. Paris: Magnard-Vuibert.

Deniz, O., Serrano, I., Bueno, G., Kim, T.K. (2014) Fast violence detection in video. *International Conference on Computer Vision Theory and Applications (VISAPP)*, pp. 478-485.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 april 2016 on the Protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing council framework decision 2008/977/JHA. Available from: https://eur-

lex.Europa.Eu/legal-content/EN/TXT/HTML/?Uri=celex:32016l0680&from=en [Accessed 24 july 2022].

Doffman, Z. (2020) Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology. *Forbes*, 26 June. Available from: https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/ [Accessed 24 July 2022].

EDPB (2019). *Guidelines 3/2019 on processing of personal data through video*. Available from: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [Accessed 24 July 2022]

Egbert, S. and Leese, M. (2020) *CRIMINAL FUTURES: predictive policing and everyday police work*. New York: Routledge, pp. 1–231.

El Naqa, I., Murphy, M.J. (2015). What Is Machine Learning?. In: El Naqa, I., Li, R., Murphy, M. (eds) *Machine Learning in Radiation Oncology*. Cham, Switzerland, Springer, pp. 3-11.

European Commission (2021). *Proposal for a Regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN [Accessed 24 July 2022].

European Union Agency for Fundamental Rights; (2020) *Getting the Future Right: Artificial Intelligence and Fundamental Rights*. Available from: https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights [Accessed 24 July 2022].

Feldstein, S. (2019) The Global Expansion of AI Surveillance. *Carnegie Endowment for International Peace*, pp. 1-42. Available from: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf [Accessed 24 July 2022].

Fernandez, JC., Mounier, L., Pachon, C. (2005). A Model-Based Approach for Robustness Testing. In: Khendek, F., Dssouli, R. (eds) *Testing of Communicating Systems. Lecture Notes in Computer Science*. 3502, pp. 333-348. Heidelberg, Germany, Springer Berlin.

Funde, N., Paranjape, P., Ram, K., Magde, P. and Dhabu, M. (2019) Object Detection and Tracking Approaches for Video Surveillance Over Camera Network. *5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, pp. 1171-1176.

Garvie, C., Bedoya, A.M. and Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown: Georgetown Law Center on Privacy & Technology, pp. 1-151. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [Accessed 24 July 2022].

Goodfellow, I, McDaniel, P and Papernot, N. (2018). Making Machine Learning Robust Against Adversarial Inputs, *Communications of the ACM*. 61(7), pp. 56-66.

Green, B., and Hu, L. (2018) The Myth in the Methodology: Towards a Recontextualization of Fairness in Machine Learning. *Presented at the Machine Learning: The Debates workshop at the 35th International Conference on Machine Learning, Stockholm, Sweden*, pp. 1-5.

Grother, P., Ngan, M., and Hanaoka, K. (2019) *Face Recognition Test (FRTV) Part 3: Demographic Effects*. National Institute of Standards and Technology, US Department of Commerce. Report: 8280.

Halder, R., Chatterjee, R. (2020) CNN-BiLSTM Model for Violence Detection in Smart Surveillance. *SN Computer Science.* 1 (201), pp. 1-9.

Hansen, L., Gad, U. P., and Petersen, K. L. (2011) The Politics of Securitization and the Muhammad Cartoon Crisis: A Post-structuralist Perspective. *Security Dialogue*. 42 (4-5), pp. 357-639.

Hill, K. (2022) Microsoft Plans to Eliminate Face Analysis Tools in Push for 'Responsible A.I.'. *New York Times*, June21. Available from: https://www.nytimes.com/2022/06/21/technology/microsoft-facial-recognition.html [Accessed 24 July 2022].

Idrees, H. and Shah, M. (2017) Enhancing camera surveillance using computer vision: a research note. *PIJPSM*. 41 (2), pp. 292-307.

Information Commissioner's Opinion. (2021) The use of live facial recognition technology in public places. Available from: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf [Accessed 24 July 2022].

IPVM. (2022) 2022 Video Surveillance 1011 Book. *IVPM*, 10 January. Available from: https://ipvm.com/reports/book-101 [Accessed 24 July 2022].

Jang, S., Battulga, L., Nasridinov, A. (2020) Detection of Dangerous Situations using Deep Learning Model with Relational Inference. *Journal of Multimedia Information System*. 7 (3), pp. 205-214.

Jenkins, R. and Purves, D. (2020) *Artificial Intelligence and Predictive Policing: A Roadmap for Research*. Available from: http://aipolicinvg.org/year-1-report.pdf [Accessed 24 July 2022].

Jha, S., Seo, C. Yang, E. Joshi, G. P. (2021) Real time object detection and tracking system for video surveillance system. *Multimedia Tools and Applications*. 80, pp.3981-3996.

Josefsson, D. (1995) William Gibson Interview. *Josefsson*.net. Available from: http://josefsson.net/gibson/ [Accessed 24 July 2022].

Joshi, A. V. (2020) *Machine Learning and Artificial Intelligence*. Cham: Switzerland.

Kaufmann, M., Egbert, S. and Leese, M. (2019) Predictive Policing and the Politics of Patterns. *The British Journal of Criminology*. 59, pp. 674-692.

Kim, D., Kim, H., Mok, Y. and Paik, J. (2021) Real-Time Surveillance System for Analyzing Abnormal Behavior of Pedestrians. *Applied Sciences*. 11 (13), pp. 1-16. https://www.mdpi.com/2076-3417/11/13/6153

Kotsiantis, S. B. (2007) Supervised Machine Learning: A Review of Classficiation Techniques. In: Breuker, J., Dieng-Kuntz, R., Guarino, N., Kok, J. N., Liu, J., Lopez de Mantaras, R., Mizoguchi, R., Musen, M. and Zhong, N. *Frontiers in Artificial Intelligence and Applications*. Amsterdam, Netherlands, IOS Press, pp. 3-24.

Koza, J.R., Bennett, F.H., Andre, D., Keane, M.A. (1996) Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. In: Gero, J.S., Sudweeks, F. (eds) *Artificial Intelligence in Design '96*. Springer, Dordrecht.

Kurakin, A., Goodfellow, I. and Bengio, S. (2017) Adversarial Machine Learning at Scale.pp. 1-17. Available from: https://arxiv.org/pdf/1611.01236.pdf [Accessed 24 July 2022].

Kwet, M. (2020). The Rise of Smart Camera Networks, and Why We Should Ban Them. *The Intercept*, 27 January. Available from: https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/ [Accessed 24 July 2022].

La Vigne, N.G., Lowry, S.S., Dwyer, A.M. and Markman, J.A. (2011). *Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners*, pp.1–59. Available from: https://www.urban.org/sites/default/files/publication/27551/412402-Using-Public-Surveillance-Systems-for-Crime-Control-and-Prevention-A-Practical-Guide-for-Law-Enforcement-and-Their-Municipal-Partners.PDF [Accessed 24 July 2022].

Leese, M. (2020) Predictive Policing: Proceed, but with Care. *Policy Perspectives*. 8 (14), pp. 1-4.

Leese, M. (2021) Security as Socio-Technical Practice: Predictive Policing and (Non-) Automation. *Swiss political science review*. 27 (1), 150-157

Leslie, D. (2020). Understanding bias in facial recognition technologies. *The Alan Turing Institute*, pp. 1-49. Available from: https://doi.org/10.5281/zenodo.4050457 [Accessed 24 July 2022].

Lindsey, S and Woolf, B. (2021). The new rules of security: How AI will transform video surveillance. *Security*, 6 April. Available from: https://www.securitymagazine.com/articles/94961-the-new-rules-of-security-how-ai-will-transform-video-surveillance [Accessed 24 July 2022].

Luo, Y. and Guo, R. (2021) Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead. *Journal of Law and Social Change*. 25 (2), pp. 153-179.

Lyon, D. (1994) *Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press.

Lyon, D. (2015) *Surveillance After Snowden*. Cambridge: Polity Press.

Mabrouk, A. B. and Zagrouba, E. (2018) Abnormal behaviour recognition for intelligent video surveillance systems: A review. *Expert Systems with Applications*. 91, pp. 480-491.

Mahtani, S and Hassan, J. (2019) Hong Kong protesters are using lasers to distract and confuse. Police are shining lights right back. *Washington Post*, 1 August. Available from: https://www.washingtonpost.com/world/2019/08/01/hong-kong-protesters-are-using-lasers-distract-confuse-police-are-pointing-them-right-back/ [Accessed 24 July 2022].

Mann, M. and Smith, M. (2017) Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *UNSW Law Journal*. 40 (1), pp. 121-145.

McCahill, M. (2007). Chapter 11: Globalisation, Surveillance and the 'War' on Terror. In: Mullard, M. and Cole, B. A. (eds.) *Globalisation, Citizenship and the War on Terror*, Cheltenham, UK, Edward Elgar Publishing.

Meel, V. (n.d.) Object Tracking in Computer Vision (Complete Guide). *viso.ai*. Available from: https://viso.ai/deep-learning/object-tracking/ [Accessed 24 July 2022].

Meijer, A., and Wessels, M. (2019) Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration*. 42 (12), pp. 1031-1039.

Milligan, C. S. (1999) Facial Recognition Technology, Video Surveillance, and Privacy. *Southern California Interdisciplinary Law Journal*. 9 (1), pp. 295-334.

Mohler, G O, Short, M B, Malinowski, S, Johnson, M, Tita, G E, Bertozzi, A L and Brantingham, P J. (2015). Randomized controlled field trials of predictive policing. *Journal of the American Statistical Association*. 110 (512), pp. 1399-1411.

Mohri, M, Rostamizadeh, A, Talwakar A (2018). *Foundations of Machine learning*. 2nd ed. Boston: MIT Press.

Ng, A. (2020). *Police will soon be able to track anywhere you drive in the US*. CNET. Available from: https://www.cnet.com/roadshow/news/license-plate-tracking-for-police-set-to-go-nationwide/ [Accessed 24 July 2022]

Noble, N. & Heale, R. (2019). Triangulation in research, with examples. *BMJ Journal.* 22 (3), pp. 67-68.

Nomerovska, I. (2021) Object Recognition, Security AI and Data Annotation. *Keymakr*, 18 November. Available from: https://keymakr.com/blog/object-recognition-security-ai-and-data-annotation/ [Accessed 24 July 2022].

Norman, T. L. (2017). Chapter 6: Electronics Elements: A detailed Discussion. In: Fennelly, L. J. (ed.). *Effective Physical Security* 5th ed, Amsterdam: Elsevier Inc.

Norton, A. A. (2013) Predictive policing: The future of law enforcement in the Trinidad and Tobago police service (TTPS). *International Journal of Computer Applications*. 62 (4), pp. 32–36.

Olatunji, I.E. and Cheng, C.-H. (2019). Video Analytics for Visual Surveillance and Applications: An Overview and Survey. *Learning and Analytics in Intelligent Systems*, pp. 475–515.

Parliamentary Office of Science and Technology (2002). P*ostnote April 2002 Number 175 CCTV*, pp. 1–4. Available from: https://www.parliament.uk/globalassets/documents/post/pn175.pdf [Accessed 24 July 2022].

Perry, W. L., McInnis, B., Price, C. C., Smith, S. and Hollywood, J. S. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND Corporation.

Podoletz, L. (2022) We have to talk about emotional AI and crime. *AI & Society*, pp. 1-16.

Porikli, F. and Yilmaz, A. (2012) Object Detection and Tracking. In: Shan, C., Porikli, F., Xiang, T., Gong, S. (eds.): *Video Analytics for Business Intelligence*. Heidelberg, Germany, Springer Berlin, pp. 3–41.

Raajmakers, S. (2019) Artificial Intelligence for Law Enforcement: Challenges and Opportunities. *IEEE Security & Privacy*. 17 (5), pp. 74-77.

Ragazzi, F., Kuskonmaz, E. M., Plajas, I., van de Ven, R., Wagner, B. (2021) *Biometric and Behavioural Mass Surveillance in EU Member States*. Report for the Greens/EFA in the European Parliament.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Accessed 24 July 2022].

Romaniuk, S. N., and Webb, T. S. (2015) Extraordinary Measures: Drone Warfare, Securitization, and the "War on Terror". *Slovak Journal of Political Sciences*. 15 (3), pp. 221-45.

Rouvroy, A. and Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth, S., Poullet, Y., Hert, P., Terwangne, C.,and Nouwt, S. (eds.) *Reinventing Data Protection?* Dordrecht, Germany, Springer, pp. 45-76.

Rychnovská, D. (2014) Securitization and the Power of Threat Framing. *Perspectives*. 22 (2), pp. 9-31.

Saikia, S., Alegre, E., Fidalgo, E., and Fernandez-Robles, L. (2017) Object Detection for Crime Scence Evidence Using Deep Learning. In: S. Battiato et al. (eds.): *ICIAP 2017, Part II, LNCS 10485*. Springer International Publishing AG, pp. 14–24.

Sandhu, A and Fussey, P. (2021) The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society*. 31 (1), pp. 66-81.

Schlehahn, E., Aichroth, P., Mann, S., Schreiner, R., Lang, U., Shepherd, I.D.H. and Wong, B.L.W. (2015). Benefits and Pitfalls of Predictive Policing. *European Intelligence and Security Informatics Conference*, pp. 1–6.

Schuetz, P. N. K. (2021) Fly in the Face of bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework. *Law & Ineq*. 39 (1), pp. 221-254.

Sherman, L. W., Gottfredson, D. C., MacKenzie, D. L., Eck, J., Reuter, P., Bushway, S. D. (1998) Preventing Crime: What Works, What Doesn't, What's Promising. *National Institute of Justice*, pp. 1-19.

Sreenu, G. and Durai, M. A. S. (2018) Intelligent video surveillance: a review through deep learning techniques for crowd analysis. *Journal of Big Data*. 6 (48), pp. 1-27.

Strikwerda, L. (2020) Predictive policing: The risks associated with risk assessment. *The Police Journal: Theory, Practice and Principles*. 94 (3), pp. 422–436.

Stritzel, H. (2007.) Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations*. 13 (3), pp. 357-83.

Sylvester, J., Raff, E. (2018). What About Applied Fairness?. *Presented at the Machine Learning: The Debates workshop at the 35th International Conference on Machine Learning 2018, Stockholm, Sweden*.

Tréguer, F. (2017) Intelligence Reform and the Snowden Paradox: The Case of France. *Media and Communication*. 5 (1), pp. 17-28.

Turner Lee, N. and Chin, C. (2022). *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*. *Brookings*. Available from: https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [Accessed 24 July 2022].

Uchida, C. (2009) *A National Discussion on Predictive Policing: Defining our Terms and Mapping Successful Implementation Strategies*. *National Institute of Justice*.

US Constitution Fourth Amendment. Available from: https://constitution.congress.gov/constitution/amendment-4/ [Accessed 24 July 2022].

Vultee, F. (201). Securitization: A new approach to the framing of the 'war on terror'. *Journalism Practice*. 4 (1), pp. 33-47.

Wendehorstc, C. and Duller, Y. (2021). *Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*. Available from: https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2021)696968 [Accessed 24 July 2022].

Yen, C. P. and Hung, T. W. (2021) Achieving Equity with Predictive Policing Algorithms: A Social Safety Net Perspective. *Science and Engineering Ethics*. 27 (36), pp. 1-16.

Zang, Q., Klette, R. (2003). Object Classification and Tracking in Video Surveillance. In: Petkov, N., Westenberg, M.A. (eds) *Computer Analysis of Images and Patterns. CAIP 2003. Lecture Notes in Computer Science* vol 2756. Heidelberg., Germany, Springe, Berlin, pp. 243-248.

Appendices

Appendix I

Document Reference	Type of Document
European Commission (2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN [Accessed 24 July 2022].	Policy/Existing legislation & regulation
Parliamentary Office of Science and Technology (2002). P*ostnote April 2002 Number 175 CCTV*.1–4. Available from: https://www.parliament.uk/globalassets/documents/post/pn175.pdf [Accessed 24 July 2022].	Policy/Existing legislation & regulation
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Accessed 24 July 2022].	Policy/Existing legislation & regulation
UK Home Office (2013). *Surveillance Camera Code of Practice*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055736/SurveillanceCameraCodePractice.pdf [Accessed 24 July 2022].	Policy/Existing legislation & regulation
US Constitution Fourth Amendment. Available from: https://constitution.congress.gov/constitution/amendment-4/ [Accessed 24 July 2022].	Policy/Existing legislation & regulation
US Constitution Fourth Amendment. Available from: https://constitution.congress.gov/constitution/amendment-1/ [Accessed 24 July 2022].	Policy/Existing legislation & regulation

CNIL (2022). *Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics position sur les conditions de déploiement*, pp. 1-18. Available from: https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Accenture and Western Digital (2018). *SEEING WHAT MATTERS A New Paradigm for Public Safety Powered by Responsible AI*, pp.1–21. Available from: https://www.accenture.com/_acnmedia/pdf-94/accenture-value-data-seeing-what-matters.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Casteel, E., Monroe, K.A., Ribeiro, P.G., Warren, R.A., Bradford Franklin, S., Onek, J.N. and Sloan, V.E. (2006). *Guidelines for Public Video Surveillance: A guide to protecting communities and preserving liberties*. Washington DC: The Constitution Project, pp. 1-60. Available from: https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
CNIL (2019). *La vidéosurveillance – vidéoprotection sur la voie publique | CNIL*. www.cnil.fr. Available from: https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique [Accessed 24 July 2022].	Policy/Report & Recommendations
Courmont, A., and Saliou, J. (2021). *La vidéosurveillance en France : des zones urbaines aux zones rurales*. LINC. Available from: https://linc.cnil.fr/fr/la-videosurveillance-en-france-des-zones-urbaines-aux-zones-rurales [Accessed 24 July 2022].	Policy/Report & Recommendations
Garante per la Protezione dei Dati Personali (2010). *Video Surveillance Guidelines by the Italian DPA*. Available from: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1767009 [Accessed 24 July 2022].	Policy/Report & Recommendations
La Vigne, N.G., Lowry, S.S., Dwyer, A.M. and Markman, J.A. (2011). *Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners*, pp.1–59. Available from:	Policy/Report & Recommendations

https://www.urban.org/sites/default/files/publication/27551/412402-Using-Public-Surveillance-Systems-for-Crime-Control-and-Prevention-A-Practical-Guide-for-Law-Enforcement-and-Their-Municipal-Partners.PDF [Accessed 24 July 2022].	
Ligue des Droits Humains (2019). *Sous l'oeil de la sécurité: la vidéo surveillance dans l'espace public*. Available from: https://www.liguedh.be/wp-content/uploads/2019/11/Brochure_LDH_Videosurveillance_2019.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Nouwt, J., de Vries, B. R., & van der Burgt, D. (2005) Camera Surveillance in the Netherlands. In: S. Nouwt, B. R. de Vries, & C. Prins (Eds.). *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*. Information Technology & Law Series 7, pp. 115-139.	Policy/Report & Recommendations
Victorian Law Enforcement Commission (2010). *Surveillance in Public Places Final Report 18* pp.1–180. Available from: https://www.lawreform.vic.gov.au/wp-content/uploads/2021/07/Surveillance_final_report.pd [Accessed 24 July 2022].	Policy/Report & Recommendations
Scylla (n.d.). *Why Law Enforcement Should Require Behavior Recognition and Anomaly Detection for Crime Prevention*. Scylla. Available from: https://www.scylla.ai/why-law-enforcement-should-require-behavior-recognition-and-anomaly-detection-for-crime-prevention/ [Accessed 24 July 2022].	Technical/Solution
Abdulghafoor, N. H., and Abdullah, H. N. (2022) A novel real-time multiple objects detection and tracking framework for different challenges. *Alexandra Engineering Journal*. 61 (12), pp. 9637-9647.	Technical/Academic
Araújo, P., Fontinele, J. and Oliveira, L. (2020) Multi-Perspective Object Detection for remote Criminal Analysis Using Drones. *IEEE Geoscience and Remote Sensing Letters*. 17 (7), pp. 1283-12816.	Technical/Academic
Funde, N., Paranjape, P., Ram, K., Magde, P. and Dhabu, M. (2019) Object Detection and Tracking Approaches for Video Surveillance Over Camera Network.*5th International Conference on Advanced*	Technical/Academic

Computing & Communication Systems (ICACCS), pp. 1171-1176.	
Idrees, H. and Shah, M. (2017) Enhancing camera surveillance using computer vision: a research note. *PIJPSM*. 41 (2), pp. 292-307.	Technical/Academic
Jang, S., Battulga, L., Nasridinov, A. (2020) Detection of Dangerous Situations using Deep Learning Model with Relational Inference. *Journal of Multimedia Information System*. 7 (3), pp. 205-214.	Technical/Academic
Jha, S., Seo, C. Yang, E. Joshi, G. P. (2021) Real time object detection and tracking system for video surveillance system. *Multimedia Tools and Applications*. 80, pp. 3981-3996.	Technical/Academic
Porikli, F. and Yilmaz, A. (2012) Object Detection and Tracking. In: Shan, C., Porikli, F., Xiang, T., Gong, S. (eds.): *Video Analytics for Business Intelligence*. Heidelberg, Germany, Springer Berlin, pp. 3–41.	Technical/Academic
Saikia, S., Alegre, E., Fidalgo, E., and Fernandez-Robles, L. (2017) Object Detection for Crime Scence Evidence Using Deep Learning. In: S. Battiato et al. (eds.): *ICIAP 2017, Part II, LNCS 10485*. Springer International Publishing AG, pp. 14–24.	Technical/Academic
Zang, Q., Klette, R. (2003). Object Classification and Tracking in Video Surveillance. In: Petkov, N., Westenberg, M.A. (eds) *Computer Analysis of Images and Patterns. CAIP 2003. Lecture Notes in Computer Science* vol 2756. Heidelberg., Germany, Springe, Berlin, pp. 243-248.	Technical/Academic
Abo Software (n.d.). *Intelligent Video Analytics Software Development*. Abto Software. Available from: https://www.abtosoftware.com/intelligent-video-analytics [Accessed 24 July 2022].	Technical/Solution
Abo Software. (2018) *Violence Detection for Smart Surveillance Systems*. Available from: https://www.abtosoftware.com/blog/violence-detection [Accessed 24 July 2022].	Technical/Solution
Boon Hui, K. and Hong Eng, K. (n.d.). *The Road to Collaborative Public Safety*. Available from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiy06a89Mr4AhXYNOwKHZlCBecQFnoECBMQAQ&url=https%3A%2F%2Fe-	Technical/Solution

file.huawei.com%2F-%2Fmedia%2FEBG%2FDownload_Files%2FPublications%2Fen%2Fsafe_city%2F07-The%2520Road%2520to%2520Collaborative%2520Public%2520Safety.pdf&usg=AOvVaw0XBL1GTJmATaEbYAzo_sPO [Accessed 24 Jul. 2022].	
Briefcam (n.d.). *Search & Review Hours of Video in Minutes*. BriefCam. Available from: https://www.briefcam.com/solutions/review-search/ [Accessed 24 Jul. 2022].	Technical/Solution
Deci (2021) The Object Detection Landscape: Accuracy vs Runtime. *Deci*, 24 May. Available from: https://deci.ai/blog/object-detection-landscape-accuracy-vs-runtime/. [Accessed 24 July 2022].	Technical/Solution
exposit (n.d.). *Computer Vision Software Development Services | CV Monitoring Software Company | CV Analytics | CV Digitization*. Exposit. Available from: https://www.exposit.com/solutions/computer-vision/ [Accessed 24 July 2022].	Technical/Solution
Flock Safety (n.d.). *Flock Safety | Eliminate Crime with Flock Safety.* Flock Safety. Available from: https://www.flocksafety.com [Accessed 24 July 2022].	Technical/Solution
Meel, V. (2021). *What is Object Tracking? - An Introduction*. viso.ai. Available from: https://viso.ai/deep-learning/object-tracking/ [Accessed 24 July 2022].	Technical/Solution
Ng, A. (2020). *Police will soon be able to track anywhere you drive in the US*. CNET. Available from: https://www.cnet.com/roadshow/news/license-plate-tracking-for-police-set-to-go-nationwide/ [Accessed 24 July 2022].	Technical/Solution
Nomerovska, I. (2021) Object Recognition, Security AI and Data Annotation. *Keymakr*, 18 November. Available from: https://keymakr.com/blog/object-recognition-security-ai-and-data-annotation/ [Accessed 24 July 2022].	Technical/Solution
Penfold, A. (2019). *How Object Recognition will boost video surveillance*. www.azena.com. Available from: https://www.azena.com/insights/how-object-recognition-will-boost-video-surveillance [Accessed 24 July 2022].	Technical/Solution

Scylla (n.d.). *Object Detection and Tracking*. Scylla. Available from: https://www.scylla.ai/object-detection-tracking/ [Accessed 24 July 2022].	Technical/Solution
Scylla (n.d.). *Report on the performance of various modules of Scylla AI Physical Threat Detection Solution*. Available from: https://f.hubspotusercontent40.net/hubfs/7561945/Lead%20Magnets/Scylla%20white%20paper.pdf?utm_medium=email&_hsmi=200674257&_hsenc=p2ANqtz-8aZWuQiWamXyiaSyVL4-RrJEgIYZmm7Yp2YsmK-MHE39KIcKbh07JtCHNNCSbAMPwBzO7zkF6Uh3sCsJ1AqxOaKFGtbtVu_TQaX6r7xcVVMYlUvHQ&utm_content=200674257&utm_source=hs_automation[Accessed 24 July 2022].	Technical/Solution
Video Surveillance - Decision dated 8 April 2010 [1734653]. Available from: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1734653[Accessed 24 July 2022].	Policy/Existing legislation & regulation
EDPB (2019). *Guidelines 3/2019 on processing of personal data through video*. Available from: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [Accessed 24 July 2022]	Policy/Existing legislation & regulation
LOI n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés. Available from: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000042563668/ [Accessed 24 July 2022].	Policy/Existing legislation & regulation

Appendix II

Document Reference	**Type of Document**
Abo Software. (2018) *Violence Detection for Smart Surveillance Systems*. Available from: https://www.abtosoftware.com/blog/violence-detection [Accessed 24 July 2022].	Technical/Solution
Accattoli, S., Sernani, P., Falcionelli, N., Mekuria, D. N., and Dragoni, A. F. (2020) Violence Detection in Videos by Combining 3D Convolutional Neural Networks and Support Vector Machines. *Applied Artificial Intelligence*. 34 (4), pp. 329-344.	Technical/Academic

Amazon (n.d.). *What is Amazon Rekognition? - Amazon Rekognition*. Available from: https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html [Accessed 24 July 2022]. INTERPOL (2017). *Facial recognition*. Interpol. Available from: https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition [Accessed 24 July 2022].	Technical/Solution
Baba, M., Gui, V., Cernazanu, C. and Pescaru, D. (2019) A Sensor Network Approach for Violence Detection in Smart Cities Using Deep Learning. *Sensors*. 19 (7).	Technical/Academic
Big Innovation Centre. (2020) *Face and Emotion Recognition Technologies: How can regulation protect citizens and their privacy?* pp.1–40. Available from: https://www.biginnovationcentre.com/wp-content/uploads/2020/07/Parliamentary-Brief-Face-and-Emotion-Recognition-Technologies-10-July-2020.pdf[Accessed 24 July 2022].	Policy/Report & Recommendations
Biometrics and Surveillance Camera Commissioner (2021). *Draft updated surveillance camera code of practice (accessible version)*. Available from: https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice/draft-updated-surveillance-camera-code-of-practice-accessible-version[Accessed 24 July 2022].	Policy/Existing legislation & regulation
Black, D. (2021) Facial analysis: automated surveillance and the attempt to quantify emotion. *Information, Communication and Society*, pp. 1-14.	Technical/Academic
Briefcam (n.d.). *Search & Review Hours of Video in Minutes*. BriefCam. Available from: https://www.briefcam.com/solutions/review-search/ [Accessed 24 July 2022].	Technical/Solution
Buolawmini, J. and Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*. 81, pp. 1-15.	Technical/Academic
Casteel, E., Monroe, K.A., Ribeiro, P.G., Warren, R.A., Bradford Franklin, S., Onek, J.N. and Sloan, V.E. (2006). *Guidelines for Public Video Surveillance: A guide to protecting communities and preserving liberties*. Washington DC: The	Policy/Report & Recommendations

Constitution Project, pp. 1-60. Available from: https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf [Accessed 24 July 2022].	
Chackravarthy, S., Schmitt, S., and Yang, L. (2018) Intelligent Crime Anomaly Detection in Smart Cities Using Deep Learning. *IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pp. 399-404.	Technical/Academic
CNIL (2022). *Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics position sur les conditions de déploiement*, pp. 1-18. Available from: https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Conger, K., Fausset, R. and Kovaleski, S.F. (2019). San Francisco Bans Facial Recognition Technology. *The New York Times*, 14 May. Available from: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [Accessed 24 July 2022].	Policy/Existing legislation & regulation (secondary)
Council of Europe. (2021) *Consultative Committee of The Convention For The Protection Of Individuals With Regard to Automatic Processing of Personal Data Convention 108: Guidelines on Facial Recognition*. Available from: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 [Accessed 24 July 2022]	Policy/Existing legislation & regulation
Deniz, O., Serrano, I., Bueno, G., Kim, T.K. (2014) Fast violence detection in video. *International Conference on Computer Vision Theory and Applications (VISAPP)*, pp. 478-485.	Technical/Academic
DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Available from: https://eur-lex.europa.eu/legal-	Policy/Existing legislation & regulation

content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN [Accessed 24 July 2022].	
Dushi, D. (2020). *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*, pp.1–12. Available from:https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content [Accessed 24 July 2022].	Policy/Report & Recommendations
EDPB (2019). *Guidelines 3/2019 on processing of personal data through video*. Available from: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [Accessed 24 July 2022]	Policy/Existing legislation & regulation
EDPB. (2022). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*. Available from: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf [Accessed 24 July 2022]	Policy/Existing legislation & regulation
European Commission (2021). *ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. Available from: https://artificialintelligenceact.eu/annexes/ [Accessed 24 July 2022].	Policy/Existing legislation & regulation
European Commission (2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN [Accessed 24 July 2022].	Policy/Existing legislation & regulation
European Commission (2022). *CORDIS | European Commission*. Europa.eu. Available from: https://cordis.europa.eu/project/id/606952/reporting [Accessed 24 July 2022].	Technical/Solution
European Union Agency for Fundamental Rights (2019). *Facial recognition technology: fundamental*	Policy/Report & Recommendations

rights considerations in the context of law enforcement, pp.1–36. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf [Accessed 24 July 2022].	
Garvie, C., Bedoya, A.M. and Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown: Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [Accessed 24 July 2022].	Technical/Academic
Gonzalez Foster, G. (2020). *Artificial Intelligence and Law Enforcement: Impacts on Fundamental Rights*, pp.1–90. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Grother, P., Ngan, M., and Hanaoka, K. (2019) *Face Recognition Test (FRTV) Part 3: Demographic Effects*. National Institute of Standards and Technology, US Department of Commerce.	Technical/Academic
Halder, R., Chatterjee, R. (2020) CNN-BiLSTM Model for Violence Detection in Smart Surveillance. *SN Computer Science.* 1 (201), pp. 1-9.	Technical/Academic
Idrees, H. and Shah, M. (2017) Enhancing camera surveillance using computer vision: a research note. *PIJPSM*. 41 (2), pp. 292-307.	Technical/Academic
Information Commissioner's Office. (2021) *The use of live facial recognition technology in public places*, pp. 1-67. Available from: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Jeffrey, D. and Paul, T. (2018). *Translation: Excerpts from China's 'White Paper on Artificial Intelligence Standardization'*. New America. Available from: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-	Policy/Existing legislation & regulation (secondary)

white-paper-artificial-intelligence-standardization/ [Accessed 24 July 2022].	
Kim, D., Kim, H., Mok, Y. and Paik, J. (2021) Real-Time Surveillance System for Analyzing Abnormal Behavior of Pedestrians. *Applied Sciences*. 11 (13), pp. 1-16. https://www.mdpi.com/2076-3417/11/13/6153	Technical/Academic
La Vigne, N.G., Lowry, S.S., Dwyer, A.M. and Markman, J.A. (2011). *Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners*, pp.1–59. Available from: https://www.urban.org/sites/default/files/publication/27551/412402-Using-Public-Surveillance-Systems-for-Crime-Control-and-Prevention-A-Practical-Guide-for-Law-Enforcement-and-Their-Municipal-Partners.PDF [Accessed 24 July 2022].	Policy/Report & Recommendations
Leslie, D. (2020). Understanding bias in facial recognition technologies. *The Alan Turing Institute*, pp. 1-49. Available from: https://doi.org/10.5281/zenodo.4050457 [Accessed 24 July 2022].	Technical/Academic
Li, P., Zhou, Z., Liu, Q., Sun, X., Chen, F., and Xue, W. (2021) Machine Learning-Based Emotional Recognition in Surveillance Video Images in the Context of Smart City Safety. *Traitement du Signal*. 38 (2), pp. 359-368.	Technical/Academic
LOI n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés. Available from: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000042563668/ [Accessed 24 July 2022].	Policy/Existing legislation & regulation
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Available from: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/ [Accessed 24 July 2022].	Policy/Existing legislation & regulation
Luo, Y., Guoi, R. (2021) Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead. *Journal of Law and Social Change*. 25 (2), pp. 153-179	Policy/Existing legislation & regulation (secondary)
Mabrouk, A. B. and Zagrouba, E. (2018) Abnormal behaviour recognition for intelligent video	Technical/Academic

surveillance systems: A review. *Expert Systems with Applications*. 91, pp. 480-491.	
Mann, M. and Smith, M. (2017) Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *UNSW Law Journal*. 40 (1), pp. 121-145.	Technical/Academic
Microsoft (2022). *Microsoft Responsible AI Standard, v2 GENERAL REQUIREMENTS*. Available from: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf [Accessed 24 July 2022].	Policy/Report & Recommendations
Milestone Systems and Oddity.AI (2022). *AI real time violence detection*. Available from: https://www.milestonesys.com/marketplace/oddity.ai/real-time-violence-detection-in-xprotect/ [Accessed 24 July 2022].	Technical/Solution
Parliamentary Office of Science and Technology (2002). P*ostnote April 2002 Number 175 CCTV*, pp. 1–4. Available from: https://www.parliament.uk/globalassets/documents/post/pn175.pdf [Accessed 24 July 2022].	Policy/Existing legislation & regulation
Perkowitz, S. (2021) The Bias in the Machine: Facial Recognition Technology and Racial Disparities. *MIT Case Studies in Social and Ethical Responsibilities of Computing*.	Technical/Academic
Podoletz, L. (2022) We have to talk about emotional AI and crime. *AI & Society*, pp. 1-16.	Technical/Academic
Popoola, O. P. and Wang, K. (2012). Video-Based Abnormal Human Behavior Recognition—A Review. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. 42 (6), 865-878.	Technical/Academic
Ragazzi, F., Kuskonmaz, E. M., Plajas, I., van de Ven, R., Wagner, B. (2021) *Biometric and Behavioural Mass Surveillance in EU Member States*. Report for the Greens/EFA in the European Parliament.	Policy/Report & Recommendations Technical/Solution
Raposo, V.L. (2022). The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research*.	Policy/Report & Recommendations

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Accessed 24 July 2022].	Policy/Existing legislation & regulation
Schuetz, P. N. K. (2021) Fly in the Face of bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework. *Law & Ineq*. 39 (1), pp. 221-254.	Technical/Academic
Scylla (n.d.). *Anomaly Detection and Behavior Recognition*. Available from: https://www.scylla.ai/anomaly-detection/ [Accessed 24 July 2022].	Technical/Solution
Scylla (n.d.). *Report on the performance of various modules of Scylla AI Physical Threat Detection Solution*. Available from: https://f.hubspotusercontent40.net/hubfs/7561945/Lead%20Magnets/Scylla%20white%20paper.pdf?utm_medium=email&_hsmi=200674257&_hsenc=p2ANqtz-8aZWuQiWamXyiaSyVL4-RrJEgIYZmm7Yp2YsmK-MHE39KIcKbh07JtCHNNCSbAMPwBzO7zkF6Uh3sCsJ1AqxOaKFGtbtVu_TQaX6r7xcVVMYlUvHQ&utm_content=200674257&utm_source=hs_automation[Accessed 24 July 2022].	Technical/Solution
Smith, M. and Miller, S. (2022) The ethical application of biometric facial recognition technology. *AI & SOCIETY*. 37, pp. 167-175.	Policy/Report & Recommendations
Sreenu, G. and Durai, M. A. S. (2018) Intelligent video surveillance : a review through deep learning techniques for crowd analysis. *Journal of Big Data*. 6 (48), pp. 1-27.	Technical/Academic
THALES (2021). *Facial recognition in 2020 (7 trends to watch)*. Available from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition [Accessed 24 Jul. 2022].	Technical/Solution

Turner Lee, N. and Chin, C. (2022). *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*. *Brookings*. Available from: https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [Accessed 24 July 2022].	Technical/Academic
Vosta, S. and Yow, K.-C. (2022) A CNN-RNN Combined Structure for Real-World Violence Detection in Surveillance Cameras. *Applied Sciences*. 12 (3).	Technical/Academic
Wendehorst, C. and Duller, Y. (2021). *Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*. Available from: https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2021)696968 [Accessed 24 July 2022].	Policy/Report & Recommendations