digital

MDPI

Article

Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police

Georgios Gkougkoudis [1,*], Dimitrios Pissanidis [2] and Konstantinos Demertzis [3]

[1] Hellenic Police, General Directorate of Attica Region, Leoforos Alexandras 173, 11522 Athens, Greece
[2] Computer Science Department, Independent Studies of Science & Technology College (IST), Sygrou Avenue 68, 11742 Athens, Greece; d.pissanidis@ist.edu.gr
[3] School of Science & Technology, Informatics Studies, Hellenic Open University, Par. Aristotelous 18, 26335 Patra, Greece; kdemertz@fmenr.duth.gr
* Correspondence: g.gkougkoudis@hellenicpolice.gr

Abstract: In the never-ending search by Law Enforcement Agencies (LEAs) for ways to reduce crime more effectively, the prevention of criminal activity is always considered the ideal solution. Since the 1990s, Intelligence-led Policing (ILP) was implemented in some forms by many LEAs around the world for crime prevention. Along with ILP, LEAs nowadays more and more turn to various new surveillance technologies. As a result, there are numerous studies and reports introducing some compelling results from LEAs that have implemented ILP, offering robust data around how the future of policing could be. In this context, this paper explores the most recent literature, identifying where ILP stands today in Greece and to what extent it could be a viable, practical approach to crime prevention. In addition, it is researched to what degree new technologies have been adopted by the European Union and the Hellenic Police in their "battle" against crime. It is concluded that most technologies are at the research stage, and studies are underway in many areas.

Keywords: policing; security; technology; surveillance; cybercrime; data analysis; AI; law enforcement

Citation: Gkougkoudis, G.; Pissanidis, D.; Demertzis, K. Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. *Digital* **2022**, *2*, 143–163. https://doi.org/10.3390/digital2020009

Academic Editors: Mirjana Ivanović, Richard Chbeir and Yannis Manolopoulos

Received: 27 November 2021
Accepted: 28 March 2022
Published: 29 March 2022

1. Introduction

Policing has gone through numerous radical changes over the years. Since the introduction of professional policing under political control in liberal democracies, various models of policing have been tested and implemented [1]. The most typical examples are Community Policing, Zero Tolerance Policing, Intelligence-Led Policing (ILP), Problem Solving Policing, Preventative Policing, Cooperative Policing, etc. [2,3]. The responsibilities and requirements of the police profession used to be simple, and the means used by the police officers, in order to perform duties, unsophisticated and "unadorned" [4]. However, since the 1930s, the policing "world" changed along with the rapid transformation of society and the development of criminality [2,4]. A significant contribution was made in this transformation of policing by J. Edgar Hoover, who introduced how science could contribute to criminal investigations, establishing, in 1932, the first Technical Crime Laboratory in the Federal Bureau of Investigations, focusing on the use of scientific analysis to solve crimes [5]. After that point, using technological innovations for collecting and analyzing criminal information and data to deal with crime and manage risk became the dominant model [2].

Security was always a multifarious subject [2,6]. Threat sources and events, crime vulnerabilities, and risks are many and diverse; thus, a lot of discussions have taken place for decades among scholars and practitioners of policing around how the modern police should respond to crime [2,6]. In this context, numerous academics and researchers [2,3,7] have stated that ILP's holistic approach that focuses on taking advantage of technology in order to accurately assess the social harm of criminality, may allow the police to prevent crime beyond borders.

One of the first and more significant steps taken towards the datafication of policing was made by the New York City Police Department in early 1994 when it introduced the Compstat system that exploited crime statistics and mapping technologies to identify crime hotspots and emerging threats [2]. The transition from an investigative ethos to a technologically driven strategic business model to address modern policing problems provided police with a real opportunity to increase its effectiveness against crime [2]. This transition was accelerated after the terrorist attacks of 9 November 2001, which revealed to the world how intelligence operations are of life-and-death importance [7]. Since that day, it was realized that homeland security and local crime prevention are not mutually exclusive; thus, the world's attention has been focused on the need for constructive changes in law enforcement intelligence [7]. That was the point where efforts focused on enhancing state and local law enforcement intelligence operations, making it possible for police to play a major role in homeland security [7]. Therefore, everyday police events and incidents were considered now crucial in the production of valuable intelligence when correlated with homeland security information. What better source for gathering information on all kinds of potential threats and vulnerabilities than police officers "on the beat" [7] (p.vii)?

The future policing environment is expected to be challenging, as it will be characterized by transnational organized criminality, global terrorism, and domestic extremism, while society will be increasingly risk concerned and influenced by intrusive media [2]. The need for convergence between criminal intelligence and national security will become imperative [2]. "Law enforcement can no longer afford to respond to contemporary and future problems with the solutions of yesterday" [7] (p.vii).

As ILP is evolving and widely applied, surveillance mechanisms are increasing [2]. In that sense, although LEAs have been implementing ILP and surveillance technologies for almost 30 years now, there is still much controversy around the use of this data-driven approach to crime prevention, as not much empirical evidence exists to either support or discredit it [8–13].

However, LEAs continue to expand their technology to obtain, retain, and search numerous non-criminal data in their effort to identify information on criminal suspects [2]. In this context, the Greek state, along with the European Union (EU), invested a lot of energy and government/EU funds on the technological upgrade of the Hellenic Police (HP) and focused on fully adopting the ILP's philosophy in everyday police work. As a result, the creation of the Aerial Means Division, the use of body-worn cameras by police officers, and innovative technological projects such as "Smart Policing" and "National Passenger Information Unit" signaled the new era that the HP has entered [14–18]. In this sense, this paper, after an extensive review of all the relevant literature, presents a broad-based study of the cutting-edge technology used by LEAs, namely the HP, in their effort to fully implement ILP and adopt its philosophy in their everyday work. However, it should be mentioned that this thorough investigation of sources showed that no significant and extensive research was realized around the subject. This fact indicates how limited the research and investigation around the new technologies that HP has or is about to adopt, has been, and how difficult it turned out to be for us to look into all the details around the theme because of the lack of previous original research data. Nevertheless, this absence of relevant research data proves the value of this research. As a result, a study researching this aspect of ILP's adoption by the HP could be considered important, offering new data in the context of the degree of the technologically driven datafication of policing in Greece.

The study is organized as follows: Section 2 describes the research design and methodology followed by the researchers; Section 3 conceptualizes the ILP doctrine and reviews related work around the new technologies implemented by LEAs in general, that have adopted ILP; Section 4 presents the EU initiatives in the same field; Section 5 presents the main results of our study on the technologies implemented or about to be adopted by the HP in its effort to apply the ILP doctrine; Section 6 gives a detailed description of the main benefits and risks that comprise from the use of such technologies; and finally the last section draws the conclusions and outlines future research directions.

2. Research Design

The general topic/title for this research paper is "Intelligence-led policing (ILP) and the new technologies in the Hellenic Police," and the research question of this study is "To what extent the new police doctrine, ILP, and new technologies are adopted by the HP?". With that in mind, the research aims to acquire knowledge around the ILP doctrine and the degree of its implementation by the HP and identifying any new technologies adopted by the EU and the HP in their effort to reduce crime. In order to achieve these aims, a review of the existing policing literature about ILP was realized in order to comprehend to what extent it is implemented by the HP. Furthermore, a thorough exploration of the existing policing and technology literature was made in order to identify technologies adopted by the EU and the HP and to contribute original data to the ongoing discussions surrounding ILP, and new police adopted technologies in Greece.

The research strategy adopted in this research can be described as a two-step procedure. The first one is collecting indirect (secondary) qualitative data from books, journals, newspaper articles, and the internet, existing data that researchers simply gather and analyze, and the second one is analyzing them using qualitative methods in order to extract valuable conclusions [19]. As a result, the research question will be best examined through conducting desk-based theoretical research [20].

This qualitative methodology was preferred due to the fact that it does not raise major ethical considerations and demand careful sampling in order to guarantee neutrality and credibility [19,21].

However, indirect data may not be custom-built for the research subject, challenging the researcher to adequately and effectively combine them in order to extract the conclusions needed [19]. In secondary data research analysis, the most important is knowing what you are looking for [19]. If the researcher knows what he/she needs, it is easier to identify adequate sources [19].

As a result, it was vital for the researchers, during the collection and analysis stage of the data, to follow some important qualitative techniques that guaranteed the objectivity and credibility of the research conclusions:

- Prolonged engagement—invest sufficient time to understand the context of each source [19];
- Persistent observation—dig further into each source, beyond an initial superficial reading [19];
- Broad representation and triangulation—collect a variety of sources of data to confirm the authenticity of each source and create a collected data sample that will be wide enough to ensure that formed conclusions are remarkable [19].

Right at this time, it should be stated that when conducting secondary research using indirect data, there is an agitation regarding the impartiality of research data collected and their sources [22,23]. As O'Leary [19] states, one's bias could "color" the data interpretations and understandings. It is vital during the analysis process to question a text's origin and the writer's agenda as some sources are by nature subjective (e.g., media coverage expressing political agendas) [19]. As a result, assessing credibility and objectivity during data collection and analysis is essential [19].

In this context, the content analysis method was used by the researchers. More specifically, the researchers moved on, carrying out an in-depth conceptual content analysis of all the data. In order to use conceptual content analysis in analyzing all the findings, we had to break them down into more manageable categories for further analysis [24,25]. As a result, the steps that were followed for the research's secondary data content analysis were as follows:

- Locating data;
- Evaluating relevance of the data;
- Assessing the credibility of the data;
- Categorizing and analyzing the data.

Through this process of content analysis, the researchers analyzed all the gathered material and tried to conceptualize and interpret it attentively, draw conclusions, and spot trends and patterns, as this type of content analysis could only quantify the information [24].

3. ILP and Technology

Globally, the intensive engagement of modern governments in the surveillance of individuals is naturally recognized as an integral part of their overall path to globalization and is closely linked to the broader socio-political conditions and the recent technological developments [26]. Although the events of 9 November 2001 are not genetically related to the already existing surveillance trend, they are nevertheless considered as a major cause of the intensification of the escalation, as most surveillance procedures, in particular the collection, distribution, and information processing, henceforth, was the most dynamic—at the same time, of course, the darkest—approach to managing the terrorist threat [7,26].

The process of legitimizing the collection and processing of information by official Law Enforcement policy bodies has begun to change dramatically, as the formal boundaries between the methods of criminal proceedings and those of the relevant state secret services have ceased to be distinguished and sometimes even to exist [1]. The British LEA, followed by its US counterparts, were the first to formally and systematically adopt a policing model based on the extensive collection of information about individuals, openly embracing very wide and frequently challenged techniques and methods of gathering information, with the aim of improving the effectiveness of counter-terrorism work [10]. At the same time, many other European countries have begun to adopt similar preventive information management practices around individuals, even before their formal involvement in the criminal justice system, only under the vague condition of probable high criminal risk [27].

This trend towards an "information-defined" form of policing, aimed at countering terrorism, soon gained the attention, not only of designers and practitioners but also of theorists and academics who began to contribute systematically to its theoretical foundation and analysis, now calling it ILP [26,28]. It soon gained strong supporters on a practical and academic level, and it was identified as one of the most important innovations of the 21st century in the field of law enforcement [26,28].

At its core, ILP can be conceptualized as a predictive model that uses the inductive method for the export of conclusions [2,7].

3.1. Defining ILP

Attempting to describe this trend presents a small difficulty in its early stages, as there is no, as one would expect, the general and universally accepted definition [2]. ILP is a "definitionally evolving concept" [2] (p. 84), and divergent interpretations of the model around the world are mainly based on the fact that it is relatively new, constantly expanding and changing, applied to jurisdictions of different cultures-necessities and with enormous room for improvement [2,26].

According to many academics [2,3,29], ILP is identified as a tool or an instrument or, as Sheptycki [29] defines it, "the technological effort to manage information about threats and risks in order to strategically manage the policing mission."

However, the recent revisions move ILP away from being a tactic or a tool and identify it as a part of a conceptual policing philosophy [2]. Ratcliffe [2], along with the Organization for Security and Co-operation in Europe (OSCE) [30], follow a more business-oriented terminology, stating that ILP is evolving into a managerial model of evidence-based resource allocation decisions through prioritization.

In most cases, ILP is described as "a strategy, a long-term and targeted approach to crime control that focuses on the identification, analysis and management of existing and growing problems or forms of risk" [3] (p. 2). According to this philosophy, the model moves more towards a problem-solving orientation of problem-oriented policing [2].

All modern definitions of ILP though emphasize the importance of collecting, analyzing and sharing information and data in the "battle" against crime [2,27]. This policing

model—inspired by the modern crime management mentality—attempts to be implemented through the systematic collection of information (not only criminological) and the analysis of relevant data in order to help formulate a more general decision-making framework, with the ultimate goal of crime reduction and prevention, both through problem management strategy and effective repression, targeting, in particular, the most dangerous criminals [28].

3.2. LEA and Technology

ILP and the technology that comes with it is transforming LEAs work in the 21st century, introducing new tools to deal with modern crime [26]. From drones and body-worn cameras to facial recognition software and artificial intelligence, new pioneering technologies are equipping LEAs with new capabilities to protect and serve civilians [31,32]. For instance, more and more police departments across the country are deploying drones and unmanned aerial vehicles (UAVs) as "eyes" in the sky to collect crime evidence or even prevent crimes from happening, functioning as a crime deterrence [32,33]. As technology continues to transform nearly every aspect of society, LEAs' leaders now have an arsenal of high-tech systems and tools that are designed to enhance public safety, catch criminals, and save lives [31,34].

After a thorough review of technology and policing literature [16–18,31–45], in order to identify the most important ILP technologies that are equipping LEAs with new capabilities to perform their duties, it can be said that these technologies are divided in 10 main categories, which are described briefly below.

3.2.1. Artificial Intelligence

The ever-growing expansion of the Internet of Things (IoT) signifies that more data are being generated, collected, and analyzed every day—much of which could be proved to be incredibly valuable for LEAs [6]. However, the process of deriving actionable insights from exploiting huge amounts of data can be incredibly time-consuming and costly when performed by police officers [2].

This Big Data challenge is recently confronted by Artificial Intelligence (AI) [8]. Technologies such as ShotSpotter, facial recognition, and biometrics contain AI algorithms [31,46]. AI is also used for crime mapping in order to more effectively pinpoint high-crime areas that should be monitored [34].

AI, in general, is mostly used by LEAs in their effort to deploy a predictive policing model. AI utilizes the so-called "deep learning" algorithms that train computers to analyze big data in order to actually predict when and where crimes are more likely to occur and help LEAs to distribute police staff accordingly to the crime hotspot areas identified [44,45].

3.2.2. Facial Recognition Software

Facial recognition capabilities came along with the development of AI that was achieved thanks to the newly introduced innovative deep learning techniques [47]. Thus, a deep learning-based face recognition system, typically when it detects a face, it starts normalizing the image and extracting facial features in order to compare them against any given face or a pool of faces existed in a database [48]. Such a system was tested for live identification of people of interest at Brussels Airport in 2017 [49].

Though advanced forms of facial recognition could prove to be a valuable tool for crime prevention with its capabilities in identifying potential terrorists and tracking criminals and missing people, such technologies are considered to be among the most controversial emerging police technologies in the 21st century [50].

3.2.3. Biometrics

In addition to fingerprints, which have been used globally for over a century, and DNA profiling, which has been used for the last 40 years by LEAs to identify criminals, now LEAs have access to an ever-expanding array of biometric and behavioral characteristics [31].

Some of the most important are emotion detection, voice recognition, gait analysis, wrist veins, iris recognition, palmprints, and even heartbeats [17,31].

For example, emotion detection technologies are used to identify the mental state and emotions of a target, examining facial expressions and other physiognomic characteristics such as gaze, voice, heart rate, body temperature, body movement, and gestures [47]. Emotion detection applications based on AI technology are already exploited in monitoring mental health, evaluating children's social and emotional skills, assessing job candidates, and detecting potential shoplifters [47].

3.2.4. Robots

In this category, one of the hottest trends is the development and construction of self-driving cars that continue to challenge the automotive industry until today [40]. This new technology was recently used by the automaker FORD to patent a self-driving police car that was equipped with artificial intelligence and was designed to identify traffic law violators by transmitting data to police officers on duty [41]. In this context, according to McGuire [30] (p.29), "the requirement for a police presence behind the wheel of patrol vehicles is itself now under threat . . . form the technology of driverless vehicles."

Moreover, there were some cases that LEAs, in order to obtain visual and audio access to specific potential crime scenes that were considered too dangerous or hard to reach, used next-generation robotic cameras, which were able to capture more complex movements and offer the level of optical resolution for close up action and consistency of coverage, space-saving and unique angles in comparison with automated cameras [42].

In the same context, a lot of ongoing research is focused on the development of police robot officers [42]. China introduced, in 2016, a security and service robot called "AnBot" that would be used to patrol banks, airports, and schools. According to Chinese Authorities [42], the "AnBot" is still under development, and in the near future, it will be deployed on the field, using facial recognition to identify criminals and was capable of following them until the police arrive [42]. In the same context, in Dubai, the Sanbot, a touchscreen-equipped robot officer that uses IBM's Watson AI system, is already on duty, patrolling tourist attractions [41]. The policing agencies in Dubai introduced this robot patrol officer in 2016, which was able to feed video to a command center, forward reported crimes to police, settle fines, run facial recognition processes, and speak nine languages. According to the United Arab Emirates Police Force, these robot officers will replace 25% of their forces by 2030 [42].

3.2.5. ShotSpotter

ShotSpotter is a new technology implemented in many cities, mainly in the United States, that detects gunfire through sensors, helping police analysts to track down the event and notify operational police officers to arrive at the scene more quickly than ever before [51]. According to Carr's research [51] in Washington and Oakland, where ShotSpotter tools were used, it was identified that only 12% of gunfire incidents resulted in a 911 call to report gunshots. However, a lot of concerns are still being raised around whether ShotSpotter can reliably distinguish the sound of gunfire from other loud, impulsive noises [52].

3.2.6. Thermal Imaging

Thermal imaging is a vastly used tool in border surveillance as it is especially effective in the dark [50]. Thermal image cameras exploit infrared imaging technology to detect heat emitted by objects such as humans and animals [36,37]. This technology is vastly used by HP in its effort to monitor and protect the borders [53]. After the migrant crisis that took place in February 2020 on the Greek-Turkish border, the HP deployed a huge number of thermal cameras, which detect human movement from body heat in a range of up to 12 km [38]. As a result, the HP monitors the movement on the border, inside the Turkish territory, in order to be prepared in case of a mass movement of people [38].

3.2.7. Automatic License (or Number) Plate Recognition (ALPR or ANPR)

The ALPR technology that is vastly used by toll collectors to automatically identify the registration numbers and letters on a car's license plate is now exploited by LEAs in their effort to identify stolen cars, arrest people with active warrants, and locate declared missing people (Amber Alerts)" [44].

This technology helped the police to automate and speed up the process of checking a license plate against LEA databases [39]. ALPR cameras are mounted at police cars and, in some cases, at streetlights, allowing LEAs to capture images of the same license plate could potentially offer the ability to track a vehicle's movements over time, which could prove to be vital in catching criminals [39].

This technology is used by the HP since 2016 in Athens and was recently deployed at the border crossings to locate both stolen vehicles and those used for illegal or criminal activities [38].

3.2.8. CCTV Systems

CCTV systems have become increasingly popular among municipalities and LEAs, as they provide important surveillance and prevention perspectives and serve as a tool for police investigation [54]. These systems are extensively exploited in London; however, the cameras used are configured to not being able to listen to conversations and capture clear pictures of public interactions [54]. They simply monitor people's behavior by covering a public space thus that it can be seen if a crime has been committed, gathering evidence at the same time ready to be used if needed, in a transubstantiation of an evidence-based policing strategy [55].

Of course, the proliferation of smartphones in the modern digital age has also exponentially increased the ability to record events, especially during police and citizen's contact [56]. As a result, video and audio recording have become a widespread integral part of the 21st-century culture [56].

In this context, video technology has been increasingly used as a surveillance mechanism, both by citizens and LEAs [6]. The first police-used video camera was introduced in the early 1990s in the US when various police patrol cars were equipped with in-car cameras that were recording real-time the police officers perform their duties [57].

3.2.9. Enhanced Body-Worn Cameras

Apart from CCTV systems and in-car cameras, body-worn police cameras that record the interactions and contacts of an on-duty police officer have also been used lately by LEAs around the world in order to provide transparency and accountability [58]. Despite the early resistance of the police personnel to the use of these cameras, research [59] showed that as accountability and transparency in the police increased, the sense of security and trust to the police officers by the citizens was augmented. A recent example of transparency was the case of George Floyd in the US, as the video recording from the police vehicle's camera was used in order to convict the police officer that shot and killed him [60,61].

This technology was recently in the center of public debate in Greece, especially after the announcements made by the Minister of Civil Protection that riot police would wear cameras to monitor the events during public demonstrations [14]. The use of body-worn cameras by the police has set in motion an ongoing debate around the importance and the impact of this technology in concepts such as privacy and data protection [14].

Nowadays, videos of police officers performing their duties in a number of high-profile incidents flood the internet and social media in an instance, drawing intense public and media scrutiny [14]. However, these videos, in most cases, do not display the whole picture of an incident as it does not depict all of the events; thus, body-worn cameras allow police supervisors and the public to gain an objective view of on-duty police work [62]. This technology, in some cases, was designed to integrate with police car systems in order to provide synchronized video of an event from multiple angles [58]. In addition, a smart holster has been developed that can activate the body-worn camera when the police officer

draws his or her firearm [14]. Moreover, there are some technological reports indicating that body-worn cameras could, in the near future, be capable of issuing an alert when an officer falls down or is hurt [58]. The facial recognition capabilities of body-worn cameras are still in the development process [31].

3.2.10. Drones

Police forces are deploying more and more drones in their everyday tasks [42]. From traffic monitoring to border control surveillance, drones have proved to be a great tool in the police's efforts against crime [42]. LEAs in certain US states have already passed legislation that allows the use of non-lethal force by robots and drones. Therefore, the US border patrol has been actively considering weaponizing its drones to immobilize potential suspects in using non-lethal force against targets of interest [42].

In that sense, the Unmanned Aircraft Service of the HP was founded in 2017 and has the responsibility of monitoring all Greek territory and transiting information to the ground police forces regarding the prevention and suppression of crime, the treatment of illegal immigration in border areas, the control of order and traffic, the support firefighters in dealing with fires, natural disasters, floods, earthquakes or serious accidents and incidents [33,35]. The Service has nine UAVs at its disposal that were recently used to monitor the traffic during quarantine hours due to COVID-19 [16,38].

In general, drones are mostly used by police to gain aerial vantage points for collecting evidence from crime scenes, crowd monitoring, and search and rescue efforts [35]. Some drones are equipped even with cameras with thermal imaging, 3D mapping, and enhanced zoom capabilities [33,35].

4. EU Initiatives

Before examining the case of HP, it is imperative to investigate the EU's involvement in adopting new police technologies as EU's decisions and actions are interconnected significantly with HP's future [63].

The EU has, for the last five years, focused its energy and resources on improving border control and mitigating security risks related to cross-border terrorism and transnational crime [47]. EU member states proved to be rather flexible in adopting new technologies that offer accurate identification of individuals in order to control mobility and reduce crime [47].

The most commonly used technology is the automated fingerprint identification technology that is currently used in three European information systems; the Schengen Information System (SIS); the European dactyloscopy database (Eurodac); and the Visa Information System (VIS) [47]. It is also about to be used in the Entry/Exit System and the European Criminal Record Information System for third-Country nationals (ECRIS-TCN) [47].

Along with fingerprint identification, DNA profiling is a new SIS feature that is expected to be fully implemented by the end of 2021 [47].

Apart from these technologies, and according to a recent study for the European Commission (EC) [64], significant opportunities were identified, all involving the use of AI such as chat bots and virtual assistants, data management and analytics tools, and risk assessment applications [64].

In this context, although not yet used, automated FRT is configured in almost all EU information systems that would allow LEAs in the near future to process facial images for identification purposes [47]. The most common example of how FRT is used in the EU is the Automated Border Control (ABC) that is deployed at the EU airports [47]. More specifically an ABC system is "an automated system which authenticates the electronic machine-readable travel document or token, establishes that the passenger is the rightful holder of the document or token, queries border control records, then determines eligibility of border crossing according to the pre-defined rules" [65]. According to FRONTEX [65], these EU ABC systems support a number of biometrics, including facial and iris recognition.

Currently, they are used only for comparing a traveler's face against the facial image of his/her travel document, thus they are about to be enhanced as soon as the biometric passports are adopted worldwide [65].

Moreover, one of the most controversial applications of AI, emotion detection technologies, although not deployed in the EU, is explored and tested in a number of EU-funded projects and initiatives for developing border control mechanisms [47].

Apart from identification processes, AI algorithms are also used by the EU for profiling persons of interest based on specific data-based risk profiles [47]. This algorithmic intelligence-driven profiling technology that assesses individual risks of security, is carried out by Member States in the framework of the Passenger Name Record (PNR) data exchange and is being developed in the context of the VIS and the European Travel Information Authorization System (ETIAS) [47].

Finally, a recent study for the EC researched the development of an AI forecasting and early warning tool for migration trends and security threats [66]. The European Asylum Support Office (EASO) has already used such a tool in order to predict the future number of asylum applications [47]. In the same context, the European Border Surveillance System (EUROSUR) that became operational in 2014 and is based on such AI forecasting technology, is now considered a well-established intelligence and risk analysis driven framework for information exchange between EU Member States and the European Border and Coast Guard Agency (Frontex) [47].

5. ILP and Technology in Greece

Technology is considered to be, along with the ILP model and information management, a mechanism for improving the efficiency and effectiveness of LEAs in relation to crime detection [67].

The ILP model, taking advantage of technology, is now a key pillar of the HP's modern anti-crime policy [2]. This approach takes place in the context of the predictive model of policing, based on processed information (intelligence); thus that the operations of the police officers could be mainly predictive—preventive and secondarily repressive [11].

The HP in its effort to implement the ILP model, allocated a lot of resources and funding mechanisms (approximately 391.465.834,73 € of EU funding) available in acquiring cutting-edge police technology that could help police officers to be more effective [68]. Furthermore, HP is experimenting with FRT and other biometric processing technologies while at the same time consolidating the use of drones for policing and border control [18].

5.1. The Role of DIDAP

One of the main representatives responsible for this effort to adopt and implement ILP by the HP is the Directorate for Management and Analysis of Intelligence (DIDAP), which was established in 2014 (Presidential Decree 178/2014). DIDAP is HP's central point of information collection, where data are evaluated, classified, and analyzed in order to identify threats and signs of high crime—crime hotspots, consolidating the predictive-led policing as a best practice [7].

In this context, DIDAP recently implemented the project for the establishment and operation of an Operational Intelligence Center through the procurement of specialized software for interconnection of databases and analysis of information related to organized crime and terrorism [27,69].

Furthermore, as of May 2018, the EU countries registered all passengers on flights to and from the EU, storing all the data in huge databases and forwarded it to the authorities of other countries [15]. In this setting, DIDAP was responsible for the implementation of another important project, aiming at the establishment of the National Passenger Information Unit (PIU) for the Development of the PNR System [15]. The PNR project was initialized after the European Council obliged all air carriers to share all passenger data (biographic information and travel route information) with the Member States [47]. The primary objective of this system is to enforce border control and prevent irregular migration

to Europe as it enables LEAs to detect unknown persons of interest before they arrive at the borders [47].

5.2. Drones and the COVID-19 Pandemic

During 2019, the HP could only use drones to monitor forests and observe traffic in motorways, was allowed to deploy drones in policing and border control activities (Presidential Decree 98/2019) [33,70]. More specifically, the Presidential Decree 98/2019 gives HP the right to use drones for any kind of policing and border control activities without a previous judicial authorization [70]. As drones are now deployed in policing and border control operations, images, and video of people's activity will be obtained [70].

In this context, HP moved on a bit further, exploiting drones during the COVID-19 pandemic [16]. According to the Hellenic Deputy Minister of Citizen Protection, Mr. Eleftherios Oikonomou, the HP used drones during the Easter holidays to ensure compliance with the movement restriction measures related to COVID-19 [33]. Many news media also reported the deployment of drones in urban areas, such as Athens and Thessaloniki, to monitor population movement [16].

Furthermore, HP has recently moved forward in procuring more UAVs and drones to augment its operational needs [33,35]. In June 2020, HP announced the acquisition of two drones through a public procurement contract of 136.000 euro, in the context of a European project called "HEFESTOS," while a few months later, the Western Greece Region concluded a contract with the HP in order to acquire drones for policing activities within the framework of the European project "INTERREG 2014–2020" [16,33,35].

5.3. Body-Worn Cameras and CCTV

The debate around the use of on-duty video recording by police officers has recently entered the Greek public discussion, after the announcements made by the Minister of Civil Protection in December 2019, about the pilot use of body-worn cameras by officers serving at the Public Order Restoration Unit and lately at the Immediate Response Unit [14,58,62]. In the same context, HP announced the realization of a project called "Smart Policing" that included the purchase and use of body-worn cameras by police officers that could identify people using Facial Recognition Technology (FRT) [17,18].

The image and sound recorded by the mobile cameras give LEAs and the public the opportunity to understand firsthand what the modern police officer is called to face during his shift [55].

Body-worn cameras can be both repressive and preventive [58]. Their primary role is of a repressive nature as the recording of video and audio carried by the police makes it easy to recall any interaction, observation or other behavior that could be used to extract useful evidence in identifying crime at an intelligence and judiciary level [58,62]. As a result, this repressive role mentioned could lead to the prevention of crime, as cameras are expected to act as police agents, capturing any misconduct on the part of both citizens and police officers [14]. As Farrar [43] (p.9) mentions "human beings can change their behavior when they know they are being observed and their movements are being recorded and are more likely to adopt more socially acceptable behavior, compliance with the rule of law and a greater sense of cooperation with the police".

In this framework, Couderta et al. [14] stated that such cameras are expected to increase the transparency of police action by documenting events that may involve police officers. This video recording documentation will serve as a reliable source of evidence of any interactions between police and citizens, exposing bad and good behavior [14]. Thus, it will prevent the misuse of violence and discrimination by the police or the violent behavior of citizens against the police [14]. Consequently, it is expected that policing will be improved, and public trust and confidence in the operation of the police will be restored to some degree, providing more public legitimacy [58].

However, many reservations exist around the use of such technology by the police, as there are concerns about privacy taking into account the issue of handling such personal

data recorded by those portable police cameras [71]. Furthermore, there are a lot of concerns raised by police unions about the changes this technology will bring in police working conditions [62]. More specifically, there were some discussions around the mental health issues and the stress of police officers that will derive from wearing such devices that will monitor their actions on a daily basis [62].

5.4. Smart Policing—Facial Recognition

The milestone of the effort of the HP to adopt ILP is considered to be the "Smart Policing" project for the implementation of which, during 2019, the HP offered 4 million euro to a global telecommunication systems vendor, funded by the Internal Security Fund (ISF) of the EC. This project will provide police officers with 1000 mobile devices equipped with integrated software enabling facial recognition and automated fingerprint identification that will help them increase their effectiveness during security checks [72]. More specifically, these mobile devices will be the size of a smartphone, and police officers will be able to use them during police stops and patrols, taking face photographs of suspects and collecting their fingerprints that will immediately be compared with data already stored in central databases for identification purposes [31].

The devices will be able to store at least 1,500,000 photos [72]. The new system will provide links to 20 national databases such as those of the Ministries of Justice, Transport, Interior and Foreign Affairs, as well as to European and global databases, such as those of Europol and Interpol [72].

According to the basic network architecture of the system, during the implementation of the project, a private access network will be created and supported by the Contractor that will be inserted between the thousands of mobile devices and the HP's network [46,73]. However, this will signify that a private corporation will have access to all the activity of these devices.

The HP's answer to these concerns was that these smart policing devices would offer a more coherent way to identify individuals, especially foreign nationals overstaying in Greece, in comparison to the current course of action that obliges police officers to bring any individual who does not carry identification documents to the nearest police station [73–75]. The HP elaborated that the processing of biometric data, such as the data collected by these devices, follows all National and European legislation and is in accordance with the HDPA directives [31].

5.5. Research Programs

As many will argue, research projects lie at the heart of innovation and make a critical contribution to the development of Europe's societies and cultures. In this context, apart from the already implemented projects and procurements of specialized technological equipment, the HP has agreed to take part in important European research programs that gather the global interest around the future of the modern police. These research projects that focus on the field of smart policing and border management are funded by the EC under the Horizon 2020 scheme "Secure societies—Protecting freedom and security of Europe and its citizens" [76].

More specifically, the research projects that the HP has been implementing until today are mostly focused on enhancing surveillance capabilities exploiting the IoT technology and improving the information and data stream management (big data analytics).

5.5.1. PREVISION

PREVISION (Prediction and Visual Intelligence for Security Information) is a project that focuses on the development of technological tools in the field of information and data stream management that will help LEAs to deal with (cyber)crime and terrorism [77–79].

The project is coordinated by the Institute of Communication and Computer Systems, a non-profit Academic Research Body established in 1989 by the Greek Ministry of Education.

The project's consortium consists of IT companies, organizations, and LEAs from all around Europe [77–79].

The project will deliver applications that will be able to integrate, fuse, and process heterogeneous data streams collected from the web-darkweb [80], video, road traffic, financial institutions, telecommunications, social network, and information security systems [77–79]. These applications aim at providing LEAs the capability to apply predictive analytics and detect anomalies [11,69].

5.5.2. DARLINE Deep AR Law Enforcement Ecosystem

DARLINE's objective is to investigate how augmented reality (AR) technology can be exploited by LEAs in order to help first responders in making more informed and rapid decisions in challenging incidents [81]. More specifically, the project aims at developing innovative AR tools that will exploit AR smart glass technology and powerful computer vision algorithms with 5G network architectures, allowing agile processing of real-time data and improving situational awareness when responding to criminal and terrorist incidents [81]. According to the project's deliverables, DARLENE will develop:

- AR glasses that will provide real-time information analysis and intelligence provision through capabilities such as facial recognition [31];
- Personalized Heads-Up Display (HUD) that will monitor the users' physiological state and improve situational awareness [75];
- Devices that will enable police officers to see through concrete walls of buildings, the locations of people [32];
- A 5G radio network for the DARLENE AR-based law enforcement ecosystem [32].

This project is coordinated by the Center for Research and Technology-Hellas, a Greek research center [81]. The project's consortium consists of IT companies and organizations from all around Europe and LEAs from Spain, Portugal, Germany, Cyprus, Lithuania, and Greece [81].

5.5.3. ROXANNE

ROXANNE will provide an analytics platform that will enhance investigation capabilities, improving identification of persons of interest by developing an integrated interface, fusing speech, text, and video processing technologies with criminal intelligence analysis [82]. The project will use speech processing exploiting multiple technologies such as speaker identification, multilingual automatic speech recognition, video and geographical meta-data processing, and network analysis [83].

The project is coordinated by the Idiap Research Institute, a non-profit foundation, Idiap was founded by the City of Martigny, the Canton du Valais, EPFL, the University of Geneva, and Swisscom [83]. The project's consortium consists of INTERPOL, IT companies, organizations, universities, and LEAs from all around Europe [83].

5.5.4. AIDA

AIDA, exploiting AI and Deep Learning (DL) techniques to big data analytics, will develop a descriptive and predictive data analytics platform along with its tools in order to detect, analyze, and prevent organized crime and terrorism [17]. With AIDA's platform, LEAs will be capable of dealing with huge amount of heterogeneous data (structured or unstructured) and data sets (text, images, videos, communication and traffic data, financial transactions, etc.), fusing them to produce raw intelligence through applications of big data processing, Machine Learning (ML), AI, predictive and visual analytics [31,79].

The project is coordinated by the private company Engineering Ingegneria Informatica SpA, and the project's consortium consists of EUROPOL, other IT companies, organizations, universities, and LEAs from all around Europe [31,79].

5.5.5. SHIELD

7SHIELD aims at providing a holistic framework to LEAs to allow the effective confrontation of complex cyber and physical threats by enabling the deployment of innovative technological solutions, taking advantage of IoT technology for cyber and physical protection such as e-fences, passive radars, and laser technologies, multimedia AI technologies from CCTV cameras and UAVs [31,84].

This framework will try to integrate all these technologies aiming at correlating all the data produced in an integral hub that will allow the holistic processing, analysis, and visualization and provide better security and cyber threat detection-protection [16,85]. For this purpose, pilot schemes will take place in Spain, Athens, and Finland in order to produce valuable intel to be used in the development process of the framework.

7SHIELD consortium is composed of 22 partners from 12 different countries. It includes Private companies, Centers of Excellence, Research and Technology Centers, Regulation Authorities, Meteorological Institutes, Law Enforcements, and Research Foundations [31,84].

5.5.6. CREST

The CREST project will deliver a platform that will use targeted monitoring, tracking, and analytics solutions, exploiting IoT technology to develop an autonomous system for better surveillance that will allow LEAs to improve operational and investigation capabilities, produce reliable crime and terrorism predictions and preventions [86,87]. CREST Project Consortium showcases an overall representation of 23 partners from 16 countries. The eight LEAs participating in the CREST project originated from eight countries. CREST consortium also comprises seven Research and Academic Institutions, seven Industry Partners, and one Civil Organization [86,87].

5.5.7. TRESSPASS (Robust Risk Based Screening and Alert System for Passengers and Luggage)

TRESSPASS aims at modernizing the way the security checks at border crossing points are carried out by transforming the old-fashioned "Rule based" security check protocol to a new "Risk based" one [88–90].

More specifically, a system will be developed that will enable efficient and reliable well-targeted passenger checks through the exploitation of biometric and sensing technologies (passport/id readers, CCTV systems, body, and cargo scanners) [89] and pre-existing systems and databases such as VIS, SIS, and PNR [88].

The project is coordinated by the National Center for Scientific Research "Demokritos" in Greece, and the project's consortium consists of other IT companies, organizations, universities, and LEAs from all around Europe [88].

5.5.8. BORDERUAS

BORDERUAS aims to facilitate effective border surveillance and prevent cross-border criminal activities by taking advantage of cutting-edge UAV technology available [35]. The project will provide the technology of combining a "lighter-than-air" UAV with sophisticated surveillance technology [33,35]. The project is coordinated by Vicomtech, an applied research technology center specialized in Artificial Intelligence, Visual Computing and Interaction, and the project's consortium consists of other IT companies, organizations, universities, and LEAs from all around Europe [35].

5.5.9. FOLDOUT

FOLDOUT focuses on the development of a system that will combine various sensors and technologies in order to penetrate and monitor border regions with dense foliage in extreme climates [38]. Foliage monitoring is an important unsolved part of border surveillance, especially in the heavily forested areas on the Greek-Turkish border in Evros [35,38].

According to the project's specifications, the system will collect events analyzing them with ML tools in order to continuously increase its detection and tracking capability [38].

The project is coordinated by the Austrian Institute of Technology, and the project's consortium brings together IT companies, organizations, universities, and LEAs from all around Europe. The HP in this project is represented by the Center of Security Studies of Greece (KEMEA), which is a scientific, consulting and research organization overseen by the Minister of Citizen Protection [38].

5.5.10. EWISA (Early Warning for Increased Situational Awareness)

This project aims at increasing intelligence in video surveillance, through the development of smart video surveillance mechanism that will exploit multiple technologies such as motion detection, face recognition, picture enhancement, object counting, pattern and anomaly recognition [47,84]. EWISA will provide better assessment and management of illegal migration flows at the Greek land borders as it will increase the operational situation awareness and enhance the reaction capacity of the land border security service of the HP [47,91].

The project is coordinated by the Center of Security Studies of Greece (KEMEA) along with the HP, and the project's consortium consists of the LEA of Spain and the Border Control Agencies of Romania and Finland [47,84].

6. Discussion

Many reports [2,3,16,29,31,47,63,64,84,92] indicate that the careful adoption of ILP and new technologies, such as Artificial Intelligence (AI), enhanced biometrics and surveillance tools, by LEAs in the context of policing, security, and border control, could offer numerous benefits that are vital for the future of modern policing.

The greatest pitfall in researching such technologies lies in the fact that there is little evidence on the scope of their application to strongly confirm both the expected benefits and risks arising from the use of police technology in the EU and Greece [8,10,11,13,16,31,84]. This is mainly due to the fact that there is no universal application of such technologies by any large-scale LEA.

As a result, from the scientific literature reviewed, there is little evidence to strongly confirm most of the expected benefits and risks arising from the use of police technology in the EU and Greece. For instance, little is known about the attitude of European citizens towards police officers who are equipped with cameras. Does technology increase citizens' trust in the police, as well as the legitimacy and transparency with which the police operate?

Therefore, there is an imperative need for further research of the subject. In this setting, the fact that all new technologies used for policing, security, and border control in Greece and the EU are mostly at a research level indicates that the EU is trying to find the silver lining between the risks and benefits of the implementation of such technologies. Thus, demonizing radical technological solutions is not the answer. LEAs should research and test such technologies and regulate their mode of implementation, in order to mitigate all the risks posed by their use [47,48,63,66,93,94]. That is why state and global efforts to control this technological upheaval is realized through the discussions initiated for regulatory initiatives [11,63,94].

6.1. Benefits

According to academics [47,58,64,84,95–99], the benefits offered by a careful adoption of new technologies in the context of policing, security, and border control, such as increased transparency, capacity to identify criminals, detect fraud and abuses, and access to relevant intel for guiding decisions, that are significant for the future of modern LEAs.

In a data-driven world, criminal activity is more and more interconnected with technology and the internet. In this context, the role of Big Data, at this point, should be underlined as through the adaptation of such technologies, a huge amount of data are generated that can be utilized to provide complete information to LEAs, leading to the successful

dismantlement of criminal groups. In addition, this approach may lead police officers to rely less on stereotypes about race and class [100]. In that sense, the use of big data by LEAs may reduce mass surveillance of minority neighborhoods and at the same time promote transparency through the exploitation of big data in order to "police the police" [89] (p.997) as digital trails are susceptible to oversight [100]. As a result, the accumulation of Big Data by LEAs could be used to make previous police practices that were based on individual-level bias disappear, providing an opportunity to increase transparency and accountability [100].

6.2. Risks

These powerful new technologies may also pose significant challenges related to their questionable reliability and accuracy that lead to multiple fundamental rights risks such as bias and discrimination, data protection and privacy, and unlawful profiling [47].

To an extent, the benefits of these technologies described above need to be carefully balanced against the significant ethical risks posed by such technologies to fundamental human rights [47,95]. Therefore, Dumbrava [36] (p. II) argues that developing and adopting powerful AI technologies without facing "pitfalls such as technological determinism and the myth of technological neutrality" would further increase the risk posed to fundamental rights, transparency, and accountability.

This unconditional adaptation of new policing technologies, according to surveillance scholars [97,98,101–104], led to the increase in surveillance that is now considered one of the major institutional dimensions of modern societies. According to Lyon [104], in these modern "surveillance societies" [103], which give room for the emergence of mass surveillance, some individuals, groups, and institutions are surveilled more than others, while different populations are monitored for different reasons and purposes.

In this context, the use of FRT, biometric identification technologies, and drones by the HP, according to the civil society, is in conflict with the fundamental human rights of privacy and data protection, while it encroaches on the freedom of expression and assembly [105]. This argument is reinforced by the fact that through the project "Smart Policing" that the HP is implementing, exploiting AI technologies, a private access network will be created and supported by the Contractor that will be inserted between the thousands of mobile devices and the HP's network [84]. This raises questions around whether a private corporation will have access to all the data collected from the operation of the "Smart Policing" system.

In many respects, the risk of increased state-sponsored societal control outweighs any alleged benefits that these technologies promise. To sum up, according to many technology- and society-related studies, technologies are now researched also from a social, political, and cultural context [74]. In that sense, if the current development of FRT is investigated only as science-driven progress, a one-sided perception is created, leaving outside important subjects such as the "securitization" of identity and the global surveillance culture built the last two decades [74]. In this context, the adoption of such technologies is often considered as a series of purely technical procedures and improvements [47]. Such an approach constructs a false sense of objectivity to technologies that separate technological advances from the broader legal, social, and ethical implications they may pose [47]. This false sense is also depicted in the fact that in order to deal with data complexity, a series of cognitive simplifications had to be made during information processing [2,7,10]. These simplifications though could "infect" the procedure and, to an extent, the decision with biases.

As a result, it should be mentioned that no technology adopted for policing is as neutral, impartial, and accurate as it claims to be. This, however, should not limit the implementation of such a model, as ILP methods such as statistical investigations, forensic laboratories, and information systems incorporate the basic assumptions about science and technology (neutrality, validity, and progress), building the image of efficiency and neutrality.

7. Conclusions

The primary aim of this paper was to provide insights on the degree of ILP's implementation by the HP while identifying the innovative police technologies used in the EU and Greece against crime. To accomplish these aims, an extensive and thorough review of the existing literature was conducted to establish a good knowledge base around the theme. This exploration of the academic discourse on the subject divulged some gaps in knowledge; presented the absence of comparable and comprehensive data; and highlighted that although police technology is something that concerns researchers, the research around its implementation and use in the EU and Greece is not vast.

The discussions around these new technologies are best depicted as a continuous "battle" between skeptics, who see technologies such as AI as tools of "destruction," and proponents of progress that see them as tools of "salvation" [47]. Both sides seem to agree though that new technologies are powerful tools that will have a significant impact on modern society [47]. The risk that lurks, however, is in assuming that, given their disruptive power, these technologies will inevitably have such consequences, regardless of what policies and restrictions we may pose to control them. In this context, a recent eu-LISA report [106] underlined that the adaptation of new technologies, such as AI, in policing, security and border control, is not a question of "if", but "when" and "to what extent".

Kuskonmaz and Guild [93] expressed interesting parallelism, lumping together the current haste to implement new digital technologies and the way humanity has addressed previous technological challenges. More specifically, they analogized the car technology to AI, underlining the fact that although cars can run really fast, it has not stopped policy makers from imposing driving speed limits for reasons of public safety [93]. Another great example of such a successful regulation posed on technological progress was realized on the non-proliferation of nuclear weapons through international agreements [47]. In that sense, it can be noted that "just because some technologies are possible, it does not mean that they should be accepted" [93].

As a result, state, and global response to the uncontrollable technological upheaval are taking form through the discussions initiated for regulatory initiatives [47,48,63,66,93,94]. In this regulatory effort, the EU mobilized funding mechanisms in order to move forward the implementation of numerous research projects, as the ones mentioned above, that would test the application of new AI and surveillance technologies in policing and border control. Through these research projects, it is aimed to locate any existing flaws and identify the risks posed by the use of such technologies by the EU LEAs.

In this context, in January 2021 the EC accepted a European Citizens' Initiative put forward by the "Reclaim Your Face" coalition, which calls for a ban on biometric mass surveillance [107]. Furthermore, in April 2021, the EC introduced a proposal for an AI act, which would classify all AI systems used in the fields of migration, asylum, and border control management as high-risk [47,107]. These "high-risk" systems will need to meet certain criteria concerning the quality of data collected, cybersecurity, human oversight, transparency, and technical documentation and record keeping accuracy [47].

As far as the HP is concerned, through the numerous EU research projects that are implemented in Greece regarding the use of new AI and surveillance technologies by the police, the Greek LEA benefits from turning into a technological hotbed of Europe.

Regarding the HP's projects that are already in the implementation phase and not at a research-level, such as the "Smart Policing", the body-worn cameras and the "PNR System," the HP has reassured multiple times that all the technologies adopted, comply with EU and INTERPOL legal and ethical frameworks and have been reviewed by internal experts and external ethics and stakeholder boards. In addition, it should be noted that the operation of DIDAP, the key police service for the ILP implementation, is supervised by a senior Prosecutor and the external control of HDPA, whose responsibility is to guarantee legality and enhance transparency.

After researching the use of these technologies by the HP, it was realized that the only technological solution used that needs further discussion is "Smart Policing". Although

the "Smart Policing" system offers a more efficient way to identify individuals, especially third country nationals overstaying in Greece, in comparison to the current procedure that obliges police officers to bring any individual who do not carry identification documents to the nearest police station, it creates an unanswered question around whether the private concessionaire of the project would have access to the data collected as the crypto channel created will operate at the company's network.

Regarding the body-worn cameras, it was never stated by HP that it would implement FRT. The cameras are just used to monitor the police officers doing their job with transparency and, if needed, to collect evidence for a crime committed either by the police or some suspected criminal [14]. Furthermore, the PNR system collects data that are already available to the HP legally through border security checks and airlines databases [15].

As far as the drones are concerned, until today, they were only used for border surveillance and monitoring riots, while recently, they were used for surveilling suspected criminals during police operations in order to collect evidence and capture them committing a crime [16]. The only drone use that was considered to be outside the criminal spectrum was during the COVID-19 pandemic [108] when the HP operated drones to monitor traffic during movement restrictions [16,61]. However, it was not used to identify cars and car holders and did not collect personal data, as the aim of the operation was to evaluate the risk of COVID-19 transmission, depending on the level of mobility of citizens [16,33].

Overall, it can be said that emergent technologies are reshaping policing. This raises serious questions on the limits of the automation of policing and whether automation will ultimately lead to an 'end' of professional police forces [42]. The proliferation of this "technological policing net" [42] is a phenomenon that raised concerns primarily in terms of its surveillance or privacy implications. However, this is only one aspect of the discussion. Increasingly concerning are the damaging effects of intensifying technologization upon the police and the public. Further discussion should be made on the impacts of replacing police forces as "visible societal guardians" [42] with more invisible forms of automated policing. This could be considered to be more corrosive for the public good than any privacy violation [42].

In that sense, the exploitation of new technologies in a data-driven [109,110] policing concept, although important for the goal of preventing crime, is only one part of the solution [10]. ILP, wherever implemented, was considered only as one segment of an overall policing strategy that included staff education [10]. In this context, people, software, and equipment need to be aligned as "the human factor is the primary driver of success" [10]. Always in the end police officers are the ones that analyze, interpret data, decide how to use it, and ensure their success [10].

Concluding, it is worth mentioning that the examination of all the related literature showed that there is still not enough evidence for the universal application of such technologies by any large-scale LEA. All new technologies used for policing, security, and border control in Greece and the EU are mostly at a research-level. Therefore, those agencies that want to proceed with the adoption of such technologies should carefully consider the ethical issues that arise and recognize that most of the claims (advantages and disadvantages) made will have to be re-tested in an implementation environment of each society, at a trial stage. In that sense, the Greek and European Panopticon is still far away.

Author Contributions: Conceptualization: G.G. and D.P.; methodology: G.G., D.P. and K.D.; validation: G.G., D.P. and K.D.; formal analysis: G.G., D.P. and K.D.; investigation: G.G. and D.P.; writing—original draft preparation: G.G.; writing—review and editing: G.G., D.P. and K.D.; supervision: D.P.; project administration: K.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Burcher, M.; Whelan, C. Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. *Police Q.* **2019**, *22*, 139–160. [CrossRef]
2. Ratcliffe, J. *Intelligence-Led Policing*; Willan Publishing: Cullompton, UK, 2008.
3. Maguire, M. Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Polic. Soc. Int. J.* **2000**, *9*, 316. [CrossRef]
4. Flanagin, A. The impact of contemporary communication and information technologies on police organizations. In *Law Enforcement, Communication and Community*; John Benjamins Publishing: Amsterdam, The Netherlands, 2002; pp. 85–106. ISBN 1588112551/9781588112552.
5. Hoover, J.E. Science, Crime Detection and the Federal Bureau of Investigation. *Stud. Lawyer J.* **1961**, *6*, 14–23.
6. Newburn, T.; Hayman, S. *Policing, Surveillance and Social Control*; Routledge: New York, NY, USA, 2012.
7. Peterson, M. *Intelligence-Led Policing: The New Intelligence Architecture*; Bureau of Justice Assistance: Washington, DC, USA, 2005.
8. Dignum, V. Ethics in artificial intelligence: Introduction to the special issue. *Ethics Inf. Technol.* **2018**, *20*, 1–3. [CrossRef]
9. Islam, Y.; Zahidul, A. Data Mining and Privacy of Social Network Sites' Users: Implications of the Data Mining Problem. *Sci. Eng. Ethics* **2015**, *21*, 941–966. [CrossRef]
10. LeCates, R. Intelligence-led Policing: Changing the Face of Crime Precention. In *Police Chief Magazine*; 2018; Available online: https://www.policechiefmagazine.org/changing-the-face-crime-prevention/ (accessed on 27 November 2021).
11. Seele, P. Predictive Sustainability Control: A review assessing the potential to transfer big data driven 'predictive policing' to corporate sustainability management. *J. Clean. Prod.* **2017**, *153*, 673–686. [CrossRef]
12. Spiegel, J. The Ethics of Virtual Reality Technology: Social Hazards and Public Policy Recommendations. *Sci. Eng. Ethics* **2018**, *24*, 1537–1550. [CrossRef]
13. Wessel, M.; Helmer, N. A Crisis of Ethics in Technology Innovation. *MIT Sloan Manag. Rev.* **2020**, *61*, 71–76.
14. Couderta, F.; Butin, D.; Le Métayer, D. Body-worn cameras for police accountability: Opportunities and risks. *Comput. Law Secur. Rev.* **2015**, *31*, 749–762. [CrossRef]
15. Bîrzu, B. Prevention, Detection, Investigation and Prosecution of Terrorist Offenses and Other Serious Crimes by Using Passenger Name Record (PNR) Data. Critical Opinions. Delege Ferenda Proposals. *Perspect. Bus. Law J.* **2016**, *5*, 195–206.
16. Wen, L.; Du, D.; Zhu, P.; Hu, Q.; Wang, Q.; Bo, L.; Lyu, S. Detection, Tracking, and Counting Meets Drones in Crowds: A Benchmark. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Nashville, TN, USA, 20–25 June 2021; pp. 7812–7821.
17. Taskiran, M.; Kahraman, N.; Erdem, C.E. Face recognition: Past, present and future (a review). *Digit. Signal Process.* **2020**, *106*, 102809. [CrossRef]
18. Rezende, I.N. Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New J. Eur. Crim. Law* **2020**, *11*, 375–389. [CrossRef]
19. O'Leary, Z. *The Essential Guide to Doing Your Research Project*; Sage Publications: London, UK, 2010.
20. Vartanian, T.P. *Secondary Data Analysis*; Oxford University Press: Oxford, UK, 2011.
21. Robson, C.; McCartan, K. *Real World Research*, 3rd ed.; Wiley: Chichester, UK, 2011.
22. Reiner, R. *The Politics of the Police*; Oxford University Press: Oxford, UK, 2000.
23. Hostli, O.R. Content Analysis. In *The Handbook of Social Psychology*; Lindzey, G., Aronson, E., Eds.; Amerind Publishing Co.: New Delhi, India, 1968; pp. 596–692.
24. Elo, S.; Kääriäinen, M.; Kanste, O.; Utriainen, K.; Pölkki, T.; Kyngäs, H. Qualitative Content Analysis: A Focus on Trustworthiness. *Sage Open* **2014**, *4*, 2158244014522633. [CrossRef]
25. Hsief, H.-F.; Shannon, S.E. Three Approaches to Qualitative Content Analysis. *Qual. Health Res.* **2005**, *15*, 1277–1288.
26. Manning, P. Information Technologies and the Police. *Crime Justice* **1992**, *15*, 349–398. [CrossRef]
27. Carter, D. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*; Michigan State University: East Lansing, MI, USA, 2009.
28. Innes, M.; Graef, R. 'The Anvil' in the Information Age: Police, Politics and Media. In *Policing: Politics, Culture and Control*; Bloomsbury Publishing: London, UK, 2012; pp. 155–172. ISBN 184731967X/9781847319678.
29. Sheptycki, J. Transnational Policing. *Can. Rev. Polic. Res.* **2005**, *1*, 1–7.
30. OSCE. *Project Report: Intelligence-Led Policing (ILP) 2017–2020*; OSCE: Vienna, Austria, 2021.
31. Nunn, S. Police technology in cities: Changes and challenges. *Technol. Soc.* **2001**, *23*, 11–27. [CrossRef]
32. Custers, B. Technology in policing: Experiences, obstacles and police needs. *Comput. Law Secur. Rev.* **2012**, *28*, 62–68. [CrossRef]
33. Wen, L.; Du, D.; Zhu, P.; Hu, Q.; Wang, Q.; Bo, L.; Lyu, S. Drone-based Joint Density Map Estimation, Localization and Tracking with Space-Time Multi-Scale Attention Network. *arXiv* **2019**, arXiv:1912.01811.
34. Schultz, P. Future is Here: Technology in Police Departments. *Police Chief* **2008**, *75*, 20–22,24,25.

35. Hayrapetyan, N.; Hakobyan, R.; Poghosyan, A.; Gabrielyan, V. Border Surveillance Using UAVs with Thermal Camera. In *Meeting Security Challenges Through Data Analytics and Decision Support*; Shahbazian, E., Rogova, G., Eds.; IOS Press: Amsterdam, The Netherlands, 2016; pp. 219–226. ISBN 1614997152/9781614997153.
36. Akula, A.; Ghosh, R.; Sardana, H.K. Thermal Imaging And Its Application In Defence Systems. In *The AIP Conference Proceedings 1391*; Predeep, P., Thakur, M., Ravi Varma, M.K., Eds.; American Institute of Physics: Kerala, India, 2011; pp. 333–335.
37. Dumpert, D.; Dirksen, S. Networked thermal imaging and intelligent video technology for border security applications. In Proceedings of the SPIE 6203, Optics and Photonics in Global Homeland Security II, Orlando (Kissimmee), FL, USA, 17–21 April 2006; Volume 6203.
38. Dijstelbloem, H. *Borders as Infrastructure: The Technopolitics of Border Control*; MIT Press: Cambridge, UK, 2021; ISBN 0262366371/9780262366373.
39. Kirby, S.; Turner, G. Think Crime, Think Car, Think ANPR: The Use of ANPR in Major Crime Investigations. *J. Homicide Major Incid. Investig.* **2007**, *3*, 35–42.
40. Joh, E. Policing Police Robots. *UCLA Law Rev. Discl.* **2016**, *64*, 516.
41. Szocik, K.; Abylkasymova, R. Ethical Issues in Police Robots. The Case of Crowd Control Robots in a Pandemic. *J. Appl. Secur. Res.* **2021**, 1–16. [CrossRef]
42. McGuire, M.R. The laughing policebot: Automation and the end of policing. *Polic. Soc.* **2021**, *31*, 20–36. [CrossRef]
43. Tanner, S.; Meyer, M. Police work and new 'security devices': A tale from the beat. *Secur. Dialogue* **2015**, *46*, 384–400. [CrossRef]
44. Tombul, F.; Cakar, B. Police use of technology to fight against crime. *Eur. Sci. J.* **2015**, *11*, 286–296.
45. Willis, J. Police Technology. In *The Handbook of Social Control*; Deflem, M., Ed.; Wiley Blackwell: Hoboken, NJ, USA, 2018.
46. Haskins, C.; Mac, R.; McDonald, L. Clearview AI Wants to Sell Its Facial Recognition Software to Authoritarian Regimes around the World. Available online: https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22 (accessed on 15 June 2021).
47. Dumbrava, C. *Artificial intelligence at EU Borders*; European Parliamentary Research Service: Brussels, Belgium, 2021.
48. Galbally Herrero, J.; Ferrara, P.; Haraksim, R.; Psyllos, A.; Beslay, L. *Study on Face Identification Technology for Its Implementation in the Schengen Information System*; Publications Office of the European Union: Luxembourg, 2019.
49. Peeters, B. *Facial Recognition at Brussels Airport: Face down in the Mud*; CiTiP Blog: Leuven, Belgium, 2020.
50. Nunn, S. Police Information Technology: Assessing the Effects of Computerization on Urban Police Functions. *Public Adm. Rev.* **2001**, *61*, 221–234. [CrossRef]
51. Carr, J.; Doleac, J.L. The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data. *SSRN Electron. J.* **2016**, *17*. [CrossRef]
52. Doucette, M.; Green, C.; Dineen, J.N.; Shapiro, D.; Raissian, K. Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties: A Longitudinal Analysis, 1999–2016. *J. Urban Health* **2021**, *98*, 609–621. [CrossRef]
53. Lambert, N.; Clochard, O. Mobile and Fatal: The EU Borders. In *Borderities and the Politics of Contemporary Mobile Borders*; Palgrave Macmillan: London, UK, 2015; pp. 119–137.
54. Goold, B.J. *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*; Oxford University Press: Oxford, UK, 2004.
55. Papadimitrakopoulos, G. Evidence-based policing (EBP) as a strategy for accomplishing police goals more effectively, the challenges EBP faces, and the prospects for it being adopted widely in Greece. In *Europe in Crisis: Crime, Criminal Justice, and the Way Forward*; Ant. N. Sakkoulas Publishers L.P.: Athens, Greece, 2017; pp. 881–899.
56. Erpenbach, M. Whole World is Watching: Camera Phones Put Law Enforcement Under Surveillance. *Law Enforc. Technol.* **2008**, *35*, 40–44.
57. Williams, C. Police Surveillance and the Emergence of CCTV in the 1960s. *Crime Prev. Community Saf.* **2003**, *5*, 27–37. [CrossRef]
58. Farrar, T. *Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras on Police Use-of-Force*; National Policing Institute: Arlington, VA, USA, 2013.
59. Pilant, L. Spotlight on In-Car Video Systems. *Police Chief* **1995**, *62*, 30–31.
60. Europol. *How COVID-19-Related Crime Infected Europe during 2020*; Europol: Den Haag, The Netherlands, 2020.
61. Knight, A.; Oriala, T. COVID-19, George Floyd and Human Security. *Afr. Secur.* **2020**, *13*, 111–115. [CrossRef]
62. Sousa, W.; Sakiyama, M.; Miethe, T. Inconsistencies in Public Opinion of Body-Worn Cameras on Police: Transparency, Trust, and Improved Police–Citizen Relationships. *Polic. A J. Policy Pract.* **2018**, *12*, 100–108. [CrossRef]
63. Renda, A.; Arroyo, J.; Fanni, R.; Laurer, M.; Sipiczki, A.; Yeung, T.; Maridis, G.; Fernandes, M.; Endrodi, G.; Milio, S.; et al. *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*; European Commission: Brussels, Belgium, 2021.
64. Deloitte. *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security*; European Commission: Brussels, Belgium, 2020.
65. Frontex. *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems*; Frontex: Warsaw, Poland, 2015.
66. Ecorys. *Feasibility Study on a Forecasting and Early Warning Tool for Migration Based on Artificial Intelligence Technology*; European Commission: Brussels, Belgium, 2020.
67. Braga, A.; Papachristos, A.; Hureau, D.M. The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-Analysis. *Justice Q.* **2014**, *31*, 633–663. [CrossRef]
68. Papadopoulos, V.; Marketakis, P.; Alexopoulos, P. *National Programme (ISF)*; Ministry of Interior: Athens, Greece, 2021.

69. Lozada, B. The Emerging Technology of Predictive Analytics: Implications for Homeland Security. *Inf. Secur. J. A Glob. Perspect.* **2014**, *23*, 118–122. [CrossRef]
70. FRA. *Coronavirus Pandemic in the EU—Fundamental Rights Implications*; Publications Office of the European Union: Luxembourg, 2020.
71. Goold, B.J. Public Area Surveillance and Police Work: The Impact of CCTV on Police Behaviour and Autonomy. *J. Surveill. Soc.* **2003**, *1*, 191–203. [CrossRef]
72. Smart Policing. Available online: https://innovation.gov.gr/en/innovationscaten/smart-policing/ (accessed on 4 November 2021).
73. FRA. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*; Publications Office of the European Union: Luxembourg, 2019.
74. Gates, K. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*; New York University Press: New York, NY, USA, 2011.
75. Barrett, L.F.; Adolphs, R.; Marsella, S.; Martinez, A.M.; Pollak, S.D. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychol. Sci. Public Interes.* **2019**, *20*, 1–68. [CrossRef] [PubMed]
76. European Commission. *Horizon Europe Strategic Plan (2021–2024)*; European Commission: Brussels, Belgium, 2021.
77. Pawlicka, A.; Choraś, M.; Kozik, R.; Pawlicki, M. First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. *Pers. Ubiquitous Comput.* **2021**. [CrossRef]
78. Pawlicki, M.; Choraś, M.; Kozik, R.; Hołubowicz, W. Missing and Incomplete Data Handling in Cybersecurity Applications. In Proceedings of the Asian Conference on Intelligent Information and Database Systems, Phuket, Thailand, 7–10 April 2021; Nguyen, N.T., Chittayasothorn, S., Niyato, D., Trawiński, B., Eds.; Springer: Cham, Switzerland, 2021; pp. 413–426.
79. Gerostathopoulos, I.; Fernández, D.M.; Zarras, A. Can Today's Machine Learning Pass Image-Based Turing Tests? In Proceedings of the International Conference on Information Security, Paris, France, 11–12 December 2019; Lin, Z., Papamanthou, C., Polychronakis, M., Eds.; Springer: Cham, Switzerland, 2019; pp. 129–148.
80. Demertzis, K.; Tsiknas, K. Darknet Traffic Big-Data Analysis and Network Management for Real-Time Automating of the Malicious Intent Detection Process by a Weight Agnostic Neural Networks Framework. *Electronics* **2021**, *10*, 781. [CrossRef]
81. Iosu, A. Improving Situational Awareness with DARLENE Augmented Reality Tools to Combat Crime and Terrorism. Available online: https://www.darleneproject.eu/improving-situational-awareness-with-darlene-augmented-reality-tools-to-combat-crime-and-terrorism/ (accessed on 8 November 2021).
82. Duszynska-Trojanowska, A. The Intelligence Cycle and the ROXANNE Platform. Available online: https://www.roxanne-euproject.org/news/blog/the-intelligence-cycle-and-the-roxanne-platform (accessed on 8 November 2021).
83. Shivam, G. Social Network Analysis for Criminology in ROXANNE. Available online: https://www.roxanne-euproject.org/news/blog/social-network-analysis-for-criminology-in-roxanne (accessed on 8 November 2021).
84. Gonzales Fuster, G. *Artificial Intelligence and Law Enforcement—Impact on Fundamental Rights*; European Parliament: Brussels, Belgium, 2020.
85. Andreadis, S.; Antzoulatos, G.; Mavropoulos, T.; Giannakeris, P.; Tzionis, G.; Pantelidis, N.; Ioannidis, K.; Karakostas, A.; Gialampoukidis, I.; Vrochidis, S.; et al. A social media analytics platform visualising the spread of COVID-19 in Italy via exploitation of automatically geotagged tweets. *Online Soc. Netw. Media* **2021**, *23*, 100134. [CrossRef]
86. Gkountakos, K.; Touska, D.; Ioannidis, K.; Tsikrika, T.; Vrochidis, S.; Kompatsiaris, I. Spatio-temporal activity detection and recognition in untrimmed surveillance videos. In Proceedings of the ACM International Conference on Multimedia Retrieval, Taipei, Taiwan, 21–24 August 2021.
87. Altobelli, C.; Johnson, E.; Forgó, N.; Napieralski, A. To Scrape or Not to Scrape? The Lawfulness of Social Media Crawling under the GDPR. In *Deep Diving into Data Protection*; Herveg, J., Ed.; Larcier: Namur, Belgium, 2021.
88. Thanos, K.G.; Kyriazanos, D.; Thomopoulos, S. TRESSPASS risk and behaviour data fusion and analysis for border crossing points security. In Proceedings of the Mediterranean Security Event (MSE) 2019, Fodele Crete, Greece, 29–31 October 2019; Springer: Berlin/Heidelberg, Germany, 2020; pp. 29–31.
89. Vora, S.; Shahriari, M.; Thomopoulos, S.; Fischer, L.; Hoch, T. A scoring algorithm for abnormal traveller behaviour in border crossing areas. In Proceedings of the Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies IV, Online, 21–25 September 2020; Volume 11542.
90. Thanos, K.G.; Kyriazanos, D.; Thomopoulos, S. Fairness-by-design dempster-shafer reasoning system. In Proceedings of the Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, Online, 12–16 April 2021; Volume 11756.
91. Israel, T. *Facial Recognition at a Crossroads: Transformation at Our Borders & Beyond*; CIPPIC: Ottawa, Canada, 2020.
92. Batabyal, A.A.; Kourtit, K.; Nijkamp, P. Technological Forecasting & Social Change A political-economy analysis of the provision of urban anti-crime technologies in a model with three cities. *Technol. Forecast. Soc. Chang.* **2020**, *160*, 120211. [CrossRef]
93. Kuskonmaz, E.M.; Guild, E. *COVID-19: A New Struggle over Privacy, Data Protection and Human Rights?* European Law Blog: Trier, Germany, 2020.
94. Flynn, M.J. *Study on Technical Requirements for Data Spaces in Law Enforcement*; European Commission: Brussels, Belgium, 2020.
95. Dintino, J.; Martens, F. *Police Intelligence Systems in Crime Control: Maintaining a Delicate Balance in a Liberal Democracy*; Charles C. Thomas: Springfield, IL, USA, 1983.

96. Drozdowski, P.; Rathgeb, C.; Dantcheva, A.; Damer, N.; Busch, C. Demographic Bias in Biometrics: A Survey on an Emerging Challenge. *IEEE Trans. Technol. Soc.* **2020**, *1*, 89–103. [CrossRef]
97. Marx, G. *Windows into the Soul: Surveillance and Society in an Age of High Technology*; University of Chicago Press: Chicago, IL, USA, 2016.
98. Marx, G. *Undercover: Police Surveillance in America*; University of California Press: Berkeley, CA, USA, 1988.
99. Rule, J. *Private Lives and Public Surveillance: Social Control in the Computer Age*; Schocken Books: New York, NY, USA, 1974.
100. Brayne, S. Big Data Surveillance The Case of Policing. *Am. Sociol. Rev.* **2017**, *82*, 977–1008. [CrossRef]
101. Ball, K.; Webster, F. *The Intensification of Surveillance: Crime, Terrorism & Warfare in the Information Age*; Pluto Press: London, UK, 2003.
102. Giddens, A. *The Consequences of Modernity*; Stanford University Press: Stanford, CA, USA, 1990.
103. Lyon, D. *The Electronic Eye: The Rise of Surveillance Society*; University of Minesota Press: Minneapolis, MN, USA, 1994.
104. Lyon, D. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*; Routledge: New York, NY, USA, 2003.
105. Rogers, C.; Scally, E.J. Police use of technology: Insights from the literature. *Int. J. Emerg. Serv.* **2018**, *7*, 100–110. [CrossRef]
106. Eu-LISA. *Artificial Intelligencein the Operational Management of Large-Scale IT Systems*; Eu-LISA: Tallinn, Estonia, 2020.
107. Europa.eu Civil Society Initiative for a Ban on Biometric Mass Surveillance Practices. Available online: https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en (accessed on 14 July 2021).
108. Demertzis, K.; Taketzis, D.; Tsiotas, D.; Magafas, L.; Iliadis, L.; Kikiras, P. Pandemic Analytics by Advanced Machine Learning for Improved Decision Making of COVID-19 Crisis. *Processes* **2021**, *9*, 1267. [CrossRef]
109. Demertzis, K.; Iliadis, L.; Pimenidis, E. Geo-AI to aid disaster response by memory-augmented deep reservoir computing. *Integr. Comput. Aided Eng.* **2021**, *28*, 383–398. [CrossRef]
110. Demertzis, K.; Iliadis, L.; Anezakis, V.-D. An innovative soft computing system for smart energy grids cybersecurity. *Adv. Build. Energy Res.* **2018**, *12*, 3–24. [CrossRef]