# Smart Policing and the Evolving Landscape of Intelligent Citie

**Dr. El. Mostafa REZRAZI[1], Mr. Monsif BEROUAL[2]**

## Abstract

The fourth industrial revolution has catalyzed the adoption of artificial intelligence (AI) and digital technologies, providing states, communities, and individuals with innovative tools to address complex challenges. Governments, particularly in technologically advanced nations, leverage AI to enhance diagnostics, conduct sophisticated analyses, and strengthen predictive capabilities, which support regulatory functions, public safety, and community security. As a result, law enforcement agencies, including "smart police," are increasingly adopting big data and analytics-based methodologies as strategic tools for crime monitoring and prevention. However, using such technologies raises critical questions about balancing public safety with the fundamental human right to privacy.

This presentation explores the legal framework governing smart policing within Europe, focusing on the updated Prüm Decisions–Prüm II since December 8, 2021. This framework facilitates cross-border data exchange and cooperation in policing, aligning with EU best practices and national regulations across European countries. Additionally, the role of Interpol in coordinating international law enforcement efforts is examined, assessing the extent to which it meets the operational needs of states in a technologically interconnected era.

1- Dr. El. Mostafa REZRAZI, Senior Fellow at the Policy Center for the New South; Professor at the FGSES, University Mohammed VI Polytechnics. Morocco.

2- Mr. Monsif BEROUAL, Ph.D. Candidate, Université Sidi Mohamed Ben Abdellah – Faculty of Taza, Morocco.

A vital aspect of this analysis is the inseparability of national, regional, and international factors in modern security management. Despite the interconnectedness, disparities in regulatory standards, technological capabilities, and infrastructure—especially between the Global North and South—still impact the effectiveness of these frameworks. This paper aims to provide an in-depth reflection on these convergences and divergences, the implications for individual privacy rights, and the future of smart policing as an evolving paradigm in new forms of law enforcement and global security.

It is essential also to mention that The "smart city" concept, with a focus on technological innovation and security, indeed gained substantial traction in Asia, particularly in Singapore, China, Japan, and South Korea. These countries have approached smart cities as highly integrated ecosystems where technology is leveraged to optimize urban management, improve efficiency, and enhance security. For example, extensive data surveillance and AI-powered infrastructure in China have been integral to its Smart City Vision, often prioritizing social management and security.

In contrast, Western countries like the US, Germany, and the UK have indeed been more cautious. While their technological advancements are highly sophisticated, they often approach smart / Intelligent city initiatives with a stronger focus on safeguarding human rights and democratic values. This caution reflects concerns about privacy, data protection, and civil liberties stemming from a more critical public discourse around surveillance and personal freedoms. Consequently, Western smart city models often prioritize transparency, data ownership, and citizen rights in ways that may not always align with the rapid, security-focused implementations observed in some Asian models.

The differentiation between Asian and Western approaches to smart city models has narrowed during and after the COVID-19 crisis. The pandemic accelerated the adoption of digital infrastructure and surveillance technologies worldwide, leading Western countries to adopt strategies that previously aligned more closely with the Asian approach.

For instance, many Western cities implemented real-time data monitoring, contact tracing, and digital health passports, which required collecting and processing personal data on a larger scale than ever before. This shift marked a notable relaxation in the West's traditionally

cautious stance, prioritizing public health and safety over some privacy concerns. Public acceptance of these technologies increased in response to the crisis, leading governments to deploy smart city tools for health management, mobility tracking, and crowd control.

While Western countries continue to emphasize data privacy and civil rights, the experience of COVID-19 has led to a more pragmatic view, recognizing the benefits of integrated digital infrastructure for emergency response. This has blurred the lines between Western and Asian models, with an emerging hybrid approach that balances technological efficiency with ongoing dialogue around democratic values and rights protection.

**Keywords:** Smart policing, artificial intelligence, digital infrastructure, privacy rights, smart cities, cross-border data exchange, surveillance technology, security, and human rights.

## Introduction

In recent years[3], there has been a rapid acceleration of scientific innovation and the adoption of digital solutions supported by artificial intelligence[4] to address the challenges faced by states, communities, and individuals. This transformation, heralded by the industrial revolution, is academically referred to as the "fourth generation of industry[5]."

3- It can be said that since the launch of the vision to build a smart world, aimed at addressing the economic crisis of 2008, this vision has gained traction with the support of the World Bank, evolving into a global strategy adopted by governments worldwide to overcome various crises through the establishment of digitization as a new approach to crisis management. For more information visit : https://www.ibm.com/smarterplanet/us/en/

4- Artificial intelligence, in its broadest sense, is defined as "the ability of computers to exhibit intelligent behavior," meaning the capacity to determine and implement the optimal choice while considering speed and immediacy in task performance. This enables decision-makers or specialists in a particular field to bypass the process of search and analysis to arrive at the appropriate choice, effectively making artificial intelligence a substitute for human reasoning in scenario planning and determining suitable options for a given situation, based on the data and information available on cyberspace and devices connected to the Internet Protocol and digital communication systems. APC, 'Global Information Society: Artificial Intelligence: Human Rights, Social Justice And Development', Sweden-USA, Association For Progressive Communications, Report, 2019. p.9.

5- for further reading see: Klaus Schawb, 'The Fourth Industrial Revolution', Switzerland, World Economic Forum, Report, 2016. Available online: https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf

This fourth generation of industry is centered on industrial modernization and the initial digitization of services and the global economy, indicating the beginning of a shift in production systems whether in trade or services toward digital manufacturing. This means transitioning the global production system toward advanced industry through the development of technologies with autonomous control[6].

This industrial transformation represented by the fourth generation of industry has led to the emergence of scientific concepts supported by artificial intelligence to manage various aspects of life, whether political, economic, industrial, environmental, or even security related, based on the principle of data storage.

To enable artificial intelligence to predict risks and thus provide possible scientific scenarios for decision-making[7], law enforcement agencies have adopted scientific knowledge as a fundamental element in their preventive policies for crime control[8]. This has highlighted the term "Big Data Analysis" as a new form of scientific knowledge for managing the investigation and criminal inquiry process to establish evidence of certain crimes and identify their perpetrators[9].

This raises the era of artificial intelligence, particularly with the example of smart policing, which brings forth questions primarily regarding the continuity of the principle of the right to privacy during law enforcement's use of big data analysis systems in crime fighting[10].

6- Klaus Schwab, 'The 4th Industrial Revolution: What It Means, How to Respond', Article, Dated On: 17th January 2016, Available Online: https://www.sciencedirect.com/science/article/pii/S2199853122002761 Last Visit: 22/04/2024.

7- Kate Robertson, Yolanda Song, & (Others), 'To Surveil and Predict : A Human Rights Analysis of Algorithmic Policing in Canada, Canada, The University of Toronto, Report, Sep 2020, p.8. Available Online : https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

8- Laura Neiva, Susana Silvag & (Others), 'The Views About Big Data Among Professionals of Police Forces : A Scoping Review of Empirical Studies', Article, Dated on : 12 Mars 2023. Available Online : https://journals.sagepub.com/doi/10.1177/14613557231166225?icid=int.sj-abstract.citing-articles.7 Last Visit : 22/04/2024.

9- Bongsu Kim, Gibum Kim, & (Others), 'Building Crime Prevention System Utilizing Big Data', Korea, Institute of Criminology and Justice, vol 1, Report, 1 Dec 2014. Available Online : https://www.kicj.re.kr/board.es?mid=a20201000000&bid=0029&list_no=12313&act=view

10- Heesung Tark, Jiwon Yoon, & (Others), 'A Preliminary Study on Building Crime Prevention System Utilizing Crime Big Data', Korea, Institute of Criminology and Justice, Vol 2, Report, 1 Dec 2016. Available Online : https://www.kicj.re.kr/board.es?mid=a20201000000&bid=0029&list_no=12357&act=view

Therefore, our issue seeks to examine the legality of smart policing practices aimed at effectively combating crime to enhance the right to security and public safety in modern smart cities, which may lead to the abuse of the right to privacy, considered a fundamental right within the universal human rights framework. The analysis of the operational performance of law enforcement, namely smart policing in our paper, through the use of big data analysis to manage the investigation process aims to establish evidence of certain crimes.

The identification of perpetrators may lead to abusing the privacy rights of suspects, causing them significant harm. This article posits that the ongoing debate between the right to security, which justifies the use of smart policing technologies in search and investigation operations, and the right to privacy, considered a fundamental right within the human rights framework, can be explained by the legislative institutions in both developed and developing countries lagging behind the rapid advancements in artificial intelligence technology. The legal framework is characterized by its slow and rigid nature, in contrast to the fast-paced and complex technological landscape, rendering legislative bodies incapable of keeping up.

Therefore, this article aims to shed light on the mechanisms and foundations of smart policing to activate urban surveillance systems by analyzing smart policing practices based on the use of big data systems in the operational performance of proactive crime monitoring, and subsequently during the occurrence of criminal activity specifically, the use of big data in criminal investigations to uncover the identities of perpetrators.

In this context, we will examine the new legal framework established by the Prum 2 Agreement[11], which came into effect on

11- The Prum Agreement was signed among EU member states for security cooperation, particularly between law enforcement agencies, in 2008. One of the key topics of this agreement is the facilitation of extensive cross-border data exchange among EU member states, allowing these security agencies to identify individuals present within their national territories through the use of data analysis technologies, whether related to criminal records, biometric identification, or other personal data. This is expected to enable law enforcement agencies to automatically monitor crime and identify perpetrators of criminal acts. For more detailed information, refer to:
The European Digital Rights (EDRI), 'Respecting Fundamental Rights in The Cross-Border Investigation of Serious Crimes', Report, September 2022. p.3. Available Online :
https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf

December 8, 2021. This agreement pertains to the automated exchange of personal data among EU member states for crime monitoring and the apprehension of individuals involved in criminal activities. This case study will help us understand the role of big data analysis systems in enhancing security and crime control within the European space.

This model will help us understand the legitimacy of law enforcement agencies using smart data analysis systems as a proactive measure for crime prevention and enhancing public safety among EU member states. To address the issue and explore the paper's hypothesis, we propose the following sections:

I. Smart policing and the enabling of urban surveillance systems

II. examination of the legal framework of the Prum 2 Decisions

III. Effectiveness and the disruption of the right to privacy

## I. Smart Policing and the enabling of Urban Surveillance Systems

The smart policing model serves as an applied mechanism within the concept of smart cities, which emphasizes the optimal use of modern technology. The European Union defines a smart city as one that "integrates the city, industry, and citizens to enhance life in urban areas through more sustainable, integrated solutions, including practical innovations, better planning, a more participatory approach, greater energy efficiency, improved transportation solutions, and smart use of information and communication technologies...etc"[12].

In this context, smart policing is a management tool within the engineering framework of smart city projects, aimed at enhancing crime prevention and control measures. This shifts the operational performance of law enforcement agencies to rely on artificial intelligence, which has the capability to predict potential threats and risks. This contributes to strengthening the foundations of law enforcement operations in urban spaces[13], enabling them to make better decisions in managing potential risks and threats based on the outcomes provided by the AI system[14].

12- Al-Khomasiyah, Saddam Muhammad, 'Smart Government: Beyond Electronic Government', United Arab Emirates, Al-Qandil Printing, Distribution, and Publishing Center, 1st edition, 2017, p. 385.

13- Frederick Zviderveen Borgeslus, 'Discrimination, Artificial Intelligence, and Algorithmic Decision Making ', The Netherlands, Directorate General of Democracy, Council European, Report, 2018.

14- Ibid, p. 17.

The effectiveness of this model is particularly evident in contemporary approaches to crime prevention[15], which emphasize the enhancement of spaces and environmental changes rather than merely focusing on changing criminal behavior[16]. This perspective starts from the idea of improving the environment to prevent crime, utilizing urban planning mechanisms aimed at crime prevention.

CPTED (Crime Prevention Through Environmental Design) focuses on environmental design to enhance the defensive capabilities of spaces according to specific standards and measures that aim to reduce opportunities for crime. This approach addresses the various dimensions of crime prevention and response within urban areas[17]. Significant transformations are taking place in the context of the fourth industrial revolution, where the perspective on crime prevention and control relies increasingly on technological means[18]. This includes the enhancement of spaces through digital communication systems and the Internet of Things (IoT)[19], which connects devices using standard Internet protocols. This process is crucial for the development of smart cities within urban planning, relying on infrastructure that facilitates communication and information sharing, allowing for the monitoring of various urban components, including roads, airports, railways, traffic hubs, seaports, and other essential infrastructure–whether in governmental or non-governmental sectors[20].

---

15- Tyla Naicker, 'An Explorative Study of Environmental Design and Crime: A Case Study of MereBank Durban', South Africa, Faculty of Applied Human Sciences, University of Kwazulu-Natal, Master Disseratation, 2021. p.20. Available Online: https://researchspace.ukzn.ac.za/handle/10413/20631 Last Visit: 05/11/2023.

16- Beulah Shekhas, & (Others), 'Theories of Crime Prevention', India, Courseware, MHRD Project, National Mission Education, p. 5. Available Online : https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S001608/P001807/M027586/ET/1521106387E-TEXT.pdf Last Visit : 05/10/2023.

17- Paul Cozens, Danielle Stefani, 'Crime Prevention and Community Safety', Article, Springer Journal, Dated On: 29 December 2022. Available Online: https://link.springer.com/article/10.1057/s41300-022-00170-0 Last Visit: 14/10/2023.

18- This refers to the integration of intelligent machines into urban life and the service performance of the city, as well as the operational performance of law enforcement agencies.

19- The Internet of Things (IoT) protocol enables these machines to communicate with each other and make decisions through digital communication systems, with their tasks defined by their operational domains and purposes in relation to the relevant authorities.

20- Al-Khomasiyah, Saddam Muhammad, Op, Cit, p.p. 381-383.

Structurally, the concept of a smart city represents a system that encompasses smart systems working together. These systems include the technologies that make up the smart city, such as high-speed networks, fiber optics, sensor networks, and both wired and wireless networks. These technologies enable the monitoring and management of the city's components through data processing and analysis, aimed at improving overall performance[21].

Therefore, it can be said that the geometric conception for approaching the smart city in the context of crime prevention and response is based on three fundamental pillars to activate the urban surveillance system, which are as follows[22]:

**1. Sensors:** This system refers to the possibility of connecting urban spaces and various locations with devices capable of sensing the space and individuals by capturing data. In the context of crime prevention, it can track the movement of individuals present in watch lists by monitoring their various electronic devices, whether mobile phones, computers, or other digital devices. Thus, these devices contribute to enabling artificial intelligence in the decision-making process through the analysis of the data provided to it[23].

**2. Surveillance Cameras:** Surveillance and monitoring in urban spaces are achieved by equipping them with cameras that operate based on the principle of managing and analyzing big data. This allows for the monitoring and tracking of individuals in watch lists through facial recognition capabilities, which can identify the identities of criminals and automatically monitor their movements, enabling law enforcement agencies to take the necessary measures against them.

**3. Immediate Interaction:** The urban surveillance system is activated by establishing a central command and coordination center, referred to as an "Operational Centre," which serves as the field communication platform connected to surveillance and sensing systems. This operational center specializes in immediate response and coordinating operations with various law enforcement agencies.

21- Ibid

22- Deirdre Toner, 'Human Rights Review of Privacy and Policing', UK, Policing Board, Report, 2021. p.p. 36-60.
Available Online:

23- for further reading see : Marijn Biesiot, Tim Jacquemard, & (Others), 'Using Sensor Data for Safety and Quality of Life', Article, Dated On : 16 January 2019.
https://www.rathenau.nl/en/digitalisering/using-sensor-data-safety-and-quality-life
Last Visit: 03/05/2024.

It monitors and reviews all alerts received automatically, which indicate the potential occurrence of criminal activity. Based on these alerts, the nature of the threats is determined, and decisions are made accordingly, taking into account strategic time management. This refers to the ability to understand and analyze potential threats in urban spaces, as well as the ability to respond immediately to apprehend individuals who may pose a threat.

To clarify the role of big data analysis in detecting crime and improving the operational performance of law enforcement agencies in efforts to reduce crime rates and conduct criminal investigations to apprehend offenders, the next section will study the European space, focusing on European security cooperation represented in the exchange of personal data. This will include a review of the Prum Framework to determine the nature of the data to be stored for crime control purposes.

## II. Examination of the Legal Framework of the Prum 2 decisions

European Union countries initiated the "Prum Agreement" for security cooperation in combating terrorism, irregular migration, and cross-border crime among EU member states. This agreement came into effect on May 27, 2005, initially including Belgium, Germany, the Netherlands, Spain, France, Luxembourg, and Austria[24]. In 2008, this initiative was incorporated into the provisions of judicial and security cooperation under Decision JHA 2008/615[25].

By the European Union, thus becoming a binding system that applies to all EU member states without exception[26].

---

24- Victor Toom, Anika Ludwig, & (Others), 'The Prum Decisions as an Aspirational Regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data', Article, Dated on: 23/03/2019.
Available Online :
https://www.sciencedirect.com/science/article/pii/S1872497319300687
Last Visit : 24/04/2024.

25- For further details, please refer to the text of the decision at the following link:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF

26- Article 33 of the Prum Decision explicitly states the implementation of Decision JHA2008/615/ and makes it binding at the EU level. For further details, please refer to the provisions of the decision. Available Online:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF

The provisions of the Prum system aim to make personal data available to security agencies within the Union, including fingerprint data, DNA profiles, information about vehicle owners, and criminal record data. These data are stored within a database system that allows law enforcement agencies to access it for the purpose of managing criminal investigations and identifying individuals involved in criminal activities. This enables security agencies to monitor their movements within EU member states, in addition to analyzing evidence at crime scenes to achieve matching results[27].

In this context, software systems have been created to store and process personal data automatically to enhance the capabilities of European law enforcement agencies in surveillance, control, investigation, and criminal inquiry. Among these systems is the "Hague" program, for example, which was agreed upon at a meeting of EU member states' G-6 interior ministers held in Germany in March 2006. This meeting included Germany, the United Kingdom, France, Italy, Spain, and Poland, to confirm the principles of the Hague program[28], which emphasizes the necessity for member states to provide personal data of their citizens as outlined in the Prum Agreement[29].

Since the implementation of this program and in the initial months following the ministerial meeting of interior ministers, law enforcement agencies in Germany and Austria worked on resolving outstanding criminal cases held by Austrian authorities. In this context, a search was conducted in the DNA database, which revealed 1,510 matches for individuals suspected of engaging in criminal activities on Austrian territory who were located in Germany. These matching cases included 41 related to murder, 885 related to robbery with violence, and 85 related to extortion[30].

---

27- European Commision, 'Study on The Feasibility of Improving Information Exchange under The Prum Decisions', Report, 2020. p.7.
Available Online:
https://www.statewatch.org/media/1385/eu-com-prum-expansion-study-final-report-5-20.pdf

28- The European Comission Committe, 'Prum : An Effective Weapon Against Terrorism and Serious Crime', London, The Lord House, Report, 2006. p.10. Available Online: https://www.statewatch.org/media/documents/news/2007/may/eu-hol-prum-report.pdf

29- Ibid, p.16.

30- According to data published by the European Commission in 2019, the Prum network provides access to over 9.2 million DNA profiles to enable law enforcement authorities to conduct investigations within EU member states. In 2019 alone, security authorities conducted approximately 2.2 million searches, which included searching through 400,000 fingerprint records, resulting in around 10,000 matches involving individuals suspected of engaging in criminal activities.

The Hague program was utilized to identify the perpetrators of terrorist attacks, including the bombing at the Maelbeek station in Brussels on March 22, 2016, which resulted in the deaths of twenty people. During the criminal investigation, firearms were found, and the relevant authorities conducted a re-examination of fingerprints and collected biological evidence to create a profile. This allowed the security authorities to conduct an automated search using the Hague program to obtain matching results. By early 2018, law enforcement agencies received matching results for three individuals, who were arrested on June 18, 2018, in the Netherlands[31].

In the wake of the industrial shift towards the era of artificial intelligence, which contributed to the emergence of independently controlled software systems and the activation of urban surveillance systems, smart city projects are being implemented to manage public spaces for crime prevention and response, as mentioned in the first section. These projects not only facilitate the automated processing of data but also create systems capable of monitoring and tracking individuals if they appear on criminal record lists, with the ability to provide alerts to law enforcement agencies[32].

In this regard, on December 8, 2021, the European Union launched the new generation of the Prum system, now referred to as " Prum 2," to update it in line with the developments of the artificial intelligence era[33].

This new "Prum 2" system is built on expanding the scope of monitoring and surveillance to include the exchange of data from modern systems captured by sensors and smart generation camera recordings, specifically facial images. This enables law enforcement agencies to identify individuals through facial recognition. Additionally, the objectives of the agreement have been broadened to include the establishment of a database for missing persons, allowing law enforcement agencies access to civil registry data for processing and analysis to achieve their goals[34]. This raises questions about the continuity of the

31- Victor Toom, Anika Ludwig, & (Others), Op. Cit.

32- Alexander Babuta, 'Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities', UK, Royal United Services Institute, RUSI Paper, September 2017. p. 6.
Available Online :
https://static.rusi.org/201709_rusi_big_data_and_policing_babuta_web.pdf

33- The European Digital Rights (EDRI), Op. Cit. p. 4.

34- Ibid.

principle of the right to privacy in light of the reliance on a system for processing and analyzing personal data for crime prevention and response. What is the relationship between access to civil registry data and the prevention of criminal threats?

Thus, we will attempt in the next section to address the question of the effectiveness and the potential suspension of the right to privacy in EU member states.

## III. Effectiveness and the Suspension of the Right to Privacy

Despite the fact that the big data analysis system has contributed to improving the operational performance of law enforcement agencies by enhancing their capabilities to identify individuals committing criminal acts and tracking their movements, thus aiding security authorities in locating them, this system has also contributed to shaping a criminal justice system that incorporates scientific principles in presenting forensic evidence for ensuring fair trials linked to prosecuting suspected offenders with scientific and objective evidence[35]. However, this does not prevent us from questioning the legitimacy of law enforcement practices in the unethical use of big data analysis systems for the purpose of preventing crime and potential criminal threats in EU member states.

This raises a significant debate regarding the practices of smart policing, which are seen as abusing of the right to privacy for citizens of EU member states, particularly concerning the unethical or malicious use against minorities, protesters, and migrants in general. This includes the exposure of their "civil" data related to ethnic, racial, and even socio-economic information, as well as political stances[36].

According to a report by the European Network Against Racism (ENAR) published in 2019[37], it was acknowledged that most law enforcement agencies in EU member states employed data analysis systems to monitor certain groups by placing them on lists of "potential

35- Frederick Zviderveen Borgeslus, Op. Cit.

36- The European Digital Rights (EDRI), Op. Cit. p. 9.

37- Patrick Williams, Eric Kind, "Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices Across Europe", Brussels, The European Network Against Racism, Report, November 2019.
Available Online :
https://www.statewatch.org/media/documents/news/2019/nov/data-driven-profiling-web-final.pdf

criminals," all while lacking any legitimate criminal foundation or legal basis for their inclusion in criminal record databases as "criminals." The report emphasized that law enforcement agencies have utilized big data analysis systems without adhering to objective standards or the scientific nature of artificial intelligence technology. Instead, their enforcement and preventive practices relied on biases and prejudices against certain groups within society.

Among the most notable cases of unethical use of big data analysis systems, we can mention the following two levels:[38]

**First:** Internal data analysis within EU member states.

- **United Kingdom and the "Matrix Gang" System:** This system allows law enforcement agencies to monitor and track minorities residing in the UK, specifically those of Asian descent and Black individuals. Based on the data revealing their personal information, security services are enabled to apprehend them in public places for the purpose of inspection.

- **Netherlands and the "400Top & 600Top" Systems:** Law enforcement agencies in the Netherlands targeted youth through the "600Top" system, while the "400Top" system was designated for minors under 16 from low-income families, who are likely to become involved in cases of assault and theft. Dutch authorities adopted a similar approach to the UK by including families of Arab descent on the list of potential criminals, with the "600Top" system including a third of families of Moroccan descent[39].

- **Austria and the "Facial Image" System:** Austrian law enforcement targeted protesters and political activists by linking surveillance cameras to a database that enables identification of individuals through facial recognition. This analysis allows security authorities to monitor and track their daily movements in public spaces.

38- Patrick Williams, Eric Kind, Op. Cit.

39- Griff Ferris, Bruno Min, & (Others), 'Automating Injustice : The Use of Artificial Intelligence and Automated Decision Making System in Criminal Justice in Europe', Fair Trials, Report. p.12.
Available Online :
https://policehumanrightsresources.org/content/uploads/2021/09/Automating_Injustice.pdf?x19059

- **France and the "PASP" System[40]:** Law enforcement agencies in France established this system to protect the values of secularism from potential terrorist threats posed by citizens of Muslim origin. This program allows law enforcement to identify these individuals in public places for monitoring and tracking their movements in the public sphere.

## Secondly: Big Data Analysis at the EU Level[41]

- **EuroDAC System:** This program was established to manage the affairs of asylum seekers by the European Union since 2000, allowing for the storage of all data related to them. This program contains all civil data, including facial images, fingerprints, the thematic reasons for seeking asylum, as well as the nationality of the individual and the country they are coming from. With the implementation of the "Prum" decisions, law enforcement agencies, alongside the Internal Affairs Agency and agencies specialized in asylum issues, gained the right to access and analyze this data using AI-supported technology to identify these "asylum seekers" in public spaces and track their movements. It is noteworthy that by 2018, more than 5,185,157 identities of asylum seekers had been stored[42].

- **EES System:** This is a system concerning the monitoring and tracking of the movement of individuals within EU member states. This procedure applies to all citizens of non-European nationalities and EU citizens with dual nationality. Through this system, law enforcement agencies will be enabled to employ big data analysis to monitor and track the identities of individuals whose travel validity has expired within Europe. This is achieved by allowing law enforcement to automatically know the expiration dates of travel documents, enabling security agencies to send alerts regarding legal violations that occur due to the expiration of the individual's legal stay. The "Entry and Exit System" program operates based on the analysis of data related to facial recognition, fingerprinting and the access to data

40- PASP : The Prevention of Public Security Attacks.

41- Chris Jones, & (Others), 'Data Protection, Immigration Enforcement Law and Fundamental Rights : What the EU's Regulations on Interoperability Mean for People with Irregular Status', Brussels, Centre of European Policy Studies, PICUM, Report, November 2019. p.p. 5-7. Available Online: https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf

42- Chris Jones, & (Others), Op. Cit. p.44.

analysis related to the reasons for entering the European Union countries[43].

These aforementioned practices can be explained by law enforcement agencies, which often relied on the framework emerging from the Schengen Area[44]. This framework expands cooperation areas to include security and judicial cooperation, ensuring crime control and the establishment of a secure European space. Therefore, we find that the European decision-making system has become stable and secure from cross-border threats[45]. The 'Prum' initiative emerged as a new tool to revive the essence of the cooperative European space and enhance institutional performance among the EU member states[46]. This led to legitimizing the large-scale exchange of personal data of citizens and visitors to the Schengen Area, as a proactive and coordinated collective measure aimed at preserving the values of the European Union and responding to various potential threats within the European space. This justifies the behaviors of law enforcement agencies, which granted themselves the right to engage in practices that exceed the right to privacy[47], controlling the system for processing and analyzing criminal and civil data automatically to prevent and combat crime.

In this context, a series of directives were issued to regulate the transfer of personal data in various classifications within the EU member states, enhancing the legitimacy of data control and thereby surpassing the right to privacy for law enforcement purposes, as follows[48]:

---

43- ibid, .50.

44- The Schengen Agreement was signed on June 14, 1985. For more information on the contents of the agreement, please visit the official website of the European Union's Internal Affairs at the following link: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-area_en

45- Sara Matos, 'Privacy and Data Protection in The Surveillance Society: The Case of The Prum System", Article, Dated on: August 2019. Available Online: https://www.sciencedirect.com/science/article/pii/S1752928X1930068X Last Visit: 30/04/2024.

46- One of the most prominent supranational institutions responsible for monitoring the transfer and availability of personal data, as well as criminal investigations, is EuroPol. For more information, please visit the official website: https://www.europol.europa.eu

47- Sara Matos, Op. Cit.

48- For further information on the regulatory laws issued by the European Council and the European Parliament to confirm the validity of the 'Prum' decisions regarding data availability to ensure security and judicial cooperation, please visit the following link: https://www.europeansources.info/record/proposal-for-a-regulation-on-automated-data-exchange-for-police-cooperation-prum-ii-amending-council-decisions-2008-615-jha-and-2008-616-jha-and-regulations-eu-2018-1726-2019-8/

The 'Prum' decisions related to the availability of data include:

- Decision 2008/615/JHA concerning DNA data access.
- Decision 2008/616/JHA concerning fingerprint access.
- Decision 2008/617/JHA concerning vehicle registration data access.
- Decision 2008/919/JHA concerning criminal record data of suspected terrorists.
- Decision EU/2019/818 concerning migrant and asylum seeker data.

However, these regulatory and directive decisions did not provide any guarantees or constraints limiting law enforcement agencies' powers in the face of unethical and unscientific use of artificial intelligence technology. This is especially concerning when discriminatory results are produced based on biased programming, as observed in previous examples. Such practices have led to the classification of individuals based on discriminatory criteria like race and religious identity, resulting in their inclusion on criminal watch lists without legal basis or evidence of wrongdoing. This highlights the slow adaptation of legal frameworks and legislative institutions to rapid technological changes, leaving room for unethical and discriminatory practices by law enforcement as they rely on digital solutions in operational performance.

## Conclusion

The legal rule and legislative time can be considered incapable of containing and absorbing technological transformations, as artificial intelligence technology differs from previous technologies; it is not characterized by stability and rigidity but relies on the ability to learn and innovate autonomously, similar to the human mind. This means that artificial intelligence has the capacity for self-construction, indicating that we are discussing a technology that will change all established principles, making it difficult to comprehend and predict.

It is expected that AI-supported technology will contribute to creating a unique human model based on scientific decision-making, which considers speed and accuracy in responding to various potential threats and risks. Thus, decisions will be based on precise data to achieve optimal responses for managing threats and reaching security objectives.

Consequently, this will lead to changes in the general principles of human rights and public freedoms, especially if programmed according to moral patterns and discriminatory standards, which could undermine the prevailing model, gradually abolishing democratic gains. This includes the complete elimination of the right to privacy and the principle of protecting personal data to respond to potential threats and prevent crime in general.

## References


✓ **Articles:**

- Biesiot Marjin, Jacquemard Tim, & (Others), 'Using Sensor Data for Safety and Quality of Life', Article, Dated On : 16 January 2019. https://www.rathenau.nl/en/digitalisering/using-sensor-data-safety-and-quality-life
- Cozens Paul, Stefani Danielle, 'Crime Prevention and Community Safety', Article, Springer Journal, Dated On: 29 December 2022. Available Online: https://link.springer.com/article/10.1057/s41300-022-00170-0
- Matos Sara, 'Privacy and Data Protection in The Surveillance Society: The Case of The Prum System", Article, Dated on: August 2019. Available Online: https://www.sciencedirect.com/science/article/pii/S1752928X1930068X
- Neiva Laura, Silvag Susana & (Others), 'The Views About Big Data Among Professionals of Police Forces : A Scoping Review of Empirical Studies', Article, Dated on : 12 Mars 2023. Available Online : https://journals.sagepub.com/doi/10.1177/14613557231166225?icid=int.sj-abstract.citing-articles.7
- Schwab Klaus, 'The 4th Industrial Revolution: What It Means, How to Respond', Article, Dated On: 17th January 2016, Available Online: https://www.sciencedirect.com/science/article/pii/S2199853122002761
- Toom Victor, Ludwig Anika, & (Others), 'The Prum Decisions as an Aspirational Regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data', Article, Dated on: 23/03/2019. Available Online : https://www.sciencedirect.com/science/article/pii/S1872497319300687

✓ **Reports:**

- APC, 'Global Information Society: Artificial Intelligence: Human Rights, Social Justice And Development', Sweden-USA, Association For Progressive Communications, Report, 2019.
- Babuta Alexander, 'Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities', UK, Royal United Services Institute, RUSI Paper, September 2017.
- Bongsu Kim, Gibum Kim, & (Others), 'Building Crime Prevention System Utilizing Big Data', Korea, Institute of Criminology and Justice, vol 1, Report, 2014.
- Borgeslus Frederick Zviderveen, 'Discrimination, Artificial Intelligence, and Algorithmic Decision Making ', The Netherlands, Directorate General of Democracy, Council European, Report, 2018.
- Ferris Griff, Min Bruno, & (Others), 'Automating Injustice : The Use of Artificial Intelligence and Automated Decision Making System in Criminal Justice in Europe', Fair Trials, Report.
- Jones Chris, & (Others), 'Data Protection, Immigration Enforcement Law and Fundamental Rights : What the EU's Regulations on Interoperability Mean for People with Irregular Status', Brussels, Centre of European Policy Studies, PICUM, Report, November 2019.
- Robertson, Yolanda Song, & (Others), 'To Surveil and Predict : A Human Rights Analysis of Algorithmic Policing in Canada, Canada, The University of Toronto, Report.
- Schawb Klaus, 'The Fourth Industrial Revolution', Switzerland, World Economic Forum, Report, 2016.
- Tark Heesung, Yoon Jiwon, & (Others), 'A Preliminary Study on Building Crime Prevention System Utilizing Crime Big Data', Korea, Institute of Criminology and Justice, Vol 2, Report,2016 .
- Toner Deirdre, 'Human Rights Review of Privacy and Policing', UK, Policing Board, Report, 2021.
- The European Digital Rights (EDRI), 'Respecting Fundamental Rights in The Cross-Border Investigation of Serious Crimes', Report, September 2022.
- The European Commision, 'Study on The Feasibility of Improving Information Exchange under The Prum Decisions', Report, 2020.

- The European Comission Committe, 'Prum : An Effective Weapon Against Terrorism and Serious Crime', London, The Lord House, Report, 2006.
- Williams Patrick, Kind Eric, "Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices Across Europe", Brussels, The European Network Against Racism, Report, November 2019.

✓ **Dissertations & Courses:**

- Naicker Tyla, 'An Explorative Study of Environmental Design and Crime: A Case Study of MereBank Durban', South Africa, Faculty of Applied Human Sciences, University of Kwazulu-Natal, Master Disseration, 2021.
- Shekhas Beulah, & (Others), 'Theories of Crime Prevention', India, Courseware, MHRD Project, National Mission Education. Available Online : https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S001608/P001807/M027586/ET/1521106387E-TEXT.pdf

✓ **Treaties & Law:**

- EU/2019/818
- Prum Decison : 2008/615/JHA
- Prum Decision : 2008/616/JHA
- Prum Decision : 2008/617/JHA