

TITLE: PRÜM II AND THE EPRIS INDEX IN EUROPE: AN ATTEMPT TO BALANCE PEOPLE'S SECURITY AND PRIVACY?

Ramona Cavalli

Research in National Institute of Statistical in Rome and Adjunct Professor at the University of Verona, Italy

ABSTRACT

In Europe, organised crime, which is increasingly globalised and operates across borders, often involving many nationalities. Organized crime groups often reflect the societies, cultures, and value systems from which they come. Just as societies across Europe are becoming increasingly interconnected and have an international perspective, so too is organised crime connected and active internationally.

Therefore, the fight against this form of crime, both national and cross-border, requires day-to-day operational cooperation, as well as an exchange of information between the law enforcement authorities of the European Member States. To effectively combat crime, police authorities must be able to exchange data in a timely manner. In this way, the EU approved in 2021 a package of reforms, which foster cross-border police cooperation and the new Prüm II Regulation approved by the European Parliament in March 2024 with the aim of promoting security for all in Europe.

This Regulation, which, among other things, provides for the automated exchange of DNA profiles, dactyloscopic data, vehicle registration data, automated exchanges of facial images and police records, should put an end to the information gaps of previous regulatory measures, and thus increase the prevention, detection and investigation of criminal offences in the EU.

However, through an examination of the main provisions of the Regulation, the Author will analyze the most important studies conducted on this issue, both social and legal, which have highlighted the danger of many provisions.

In particular, in this study the Author will demonstrate that, although the security of European citizens is a legitimate and fundamental priority for the Commission, successfully implemented by a series of reforms aimed at fostering cross-border police cooperation including the new Prüm II Regulation, nevertheless the latter fails to produce improvements in terms of the rules of Directive 2016/680, on the protection of personal data with regard to the processing of data by police and criminal justice authorities. In fact, many of its new rules create further serious risks for the fundamental rights of the citizens themselves, with the consequent need for further new regulatory changes.

KEYWORDS

Prüm, Epris, data, security, privacy

1. INTRODUCTION: THE NEW EUROPEAN REGULATIONS AGAINST NATIONAL AND TRANSNATIONAL ORGANIZED CRIME

Since 2000, the United Nations Convention against Transnational Organized Crime has provided an internationally agreed definition of an organized crime group as "*a group of three or more persons who have existed for a certain period of time and who act in concert for the purpose of committing crimes for financial or other material benefit*"¹. This definition, also adopted in the Council of the EU Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, continues to reflect the conceptualisation of organised crime by law enforcement authorities around the world. However, this simplistic definition does not consider the complex and flexible nature of modern organized crime networks, which adapt quickly to exploit new victims, evade countermeasures, or identify new criminal opportunities².

In 2005, Belgium, France, Germany, the Netherlands, Spain, Luxembourg and Austria signed the Prüm Treaty to increase coordination measures between police and judicial authorities in the field of judicial investigations and the prevention of terrorism, transnational crime and illegal immigration, with the aim of exchanging data on the DNA and fingerprints of those convicted of criminal offences on the territory of the acceding countries. These kinds of powers, which are not provided for in the Schengen Treaty, expanded both the amount and the type of information that could be exchanged between police forces.

In addition, the agreement provided for a more in-depth exchange of information on suspects, vehicles, and the falsification of documents, as well as the possibility of creating international police teams to patrol border areas. The treaty also dealt with illegal immigration, listing a series of provisions to facilitate the identification and repatriation of people without residence permits, as well as to prevent the phenomenon, cooperating with the countries of origin.

In this way, the signatory States had in practice reciprocal access to the national databases containing the data mentioned above and could carry out searches in an automated manner. When a hit, or correspondence, occurred, the Contracting Member States could obtain the personal information associated with the hit. This system, therefore, moved away from the information tools provided for by the Schengen and Europol Implementing Conventions, based on the mechanism of mediation of the request to a central service to which the national databases are connected, approaching, instead, the innovative approach in the exchange of information between the police and judicial authorities of the Member States, contained in the Hague Programme adopted by the European Council on 4 November 2004³.

The Prüm I Treaty was signed in 2005, therefore, before the Lisbon Treaty of 2009, and even before the EU Directive 680/2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offences falling within the competence of the police or the execution of criminal penalties, as well as the free movement of such data (called the Law Enforcement Directive LED)⁴.

Originally, the Prüm framework was based on voluntary participation, while in 2008 the Council on Police and Judicial Cooperation codified an intergovernmental treaty (Prüm Convention, 2005), which allowed Member States to share data bilaterally across borders. However, this too had entered into force before the EU's Lisbon Treaty and, therefore, the original Prüm decisions did not follow the decision-making process, so that the European Parliament's role in examining the Prüm Law was very limited⁵.

Looking at the statistical data of the SOCTA report conducted by Europol in 2017, in particular, it emerged that in Europe every year about 75 million people were victims of crime⁶. On the contrary, already in 2017 more than 5,000 serious organized criminal groups were investigated in Europe, of which 7 out of 10 organized crime groups were active in more than 3 countries and collectively involved more than 180 nationalities⁷.

Thus, not only the existence and activity of transnational crime in Europe was proved, but also the use of new technologies in the modus operandi by organised crime groups (COGs).

through Europol's largest ever collection of data, through strategic agreements with Member States, Europol's operational and strategic partners outside the EU and our institutional partners, as well as operational intelligence data stored in Europol's databases. This forward-looking study found that these criminal activities were more relevant to cybercrime, including encrypted communication, trafficking in human beings, migrant smuggling, drug trafficking and excise fraud⁸.

However, already between 2012 and 2013 the EU had launched a specific four-year programming of an operational and integrated approach to internal security⁹, which presupposed and used different instruments, including external border and police controls, information management and exchange, prevention¹⁰ and the 'external' projection of the Union's internal security, including through public-private partnerships, under the 'European Multidisciplinary Platform against Criminal Threats' (EMPACT).

In 2021 the Council of the Union established ten priority areas for EMPACT 2022-2025, all of which are characterised as a danger to the internal security of the Union.

The implementation of the plan, then, involves four steps, in which the first can be identified in the "European Union Serious and Organised Crime Threat Assessment" (EU SOCTA), carried out by EUROPOL, based on which the Council of the European Union defines the priorities relating to "serious and organised crime" which plays a "key role" in EMPACT. The second step, then, involves the identification of a more limited number of priorities by the Council itself, with the preparation of a multiannual general plan with horizontal strategic objectives. It explicitly involves the use of preventive as well as repressive measures. The third step involves the development and monitoring of operational plans by the Standing Committee on Operational Cooperation on Internal Security (COSI), adopted annually and monitored by it. The last step is an independent evaluation of the effectiveness of the entire plan.

Following the path taken by SOCTA, the Commission in July 2020¹¹ He presented the "New Security Union Strategy", which includes the adoption of an agenda to tackle organized crime, including human trafficking. The two strategies ("EU Strategy to Tackle Organised Crime 2021-2025" and the "EU Strategy on Combating Trafficking in Human Beings 2021-2025"), then, were adopted in April 2021, which highlight the impressive expansion of illegal online activities brought about by the Covid-19 epidemic¹².

Examination of these legislative proposals has also revealed the possibility for the Commission to adopt an act of secondary legislation, precisely to structure EMPACT, to guide operational cooperation in preventing and combating organised crime¹³.

Given the effectiveness of EMPACT, in 2021 EU countries made it a permanent tool in the fight against organised crime and serious crime, through four-year cycles, starting with the assessment of criminal threats and the adoption of EU crime-fighting priorities. For each of these priorities, annual operational action plans are developed, implemented and monitored. Finally, an

independent evaluation is carried out at the end of the four-year cycle to assess the implementation and results of EMPACT, as well as to feed into the next cycle¹⁴. The system is structured through joint operational actions aimed at identifying criminal networks, their structures and economic models, and involves all Member States, agencies and other EU partners, which work together on a permanent basis in the framework of EMPACT to address major criminal threats.

Through all these tools, 9922 arrests were recorded in Europe in 2022, 4019 victims of human trafficking identified, 3646 migrant smugglers arrested, more than €180 million seized, more than 62 tons of drugs seized, and 9262 investigations opened¹⁵. Currently, there are also legislative initiatives by the Council aimed at amending and strengthening the existing minimum standards of the Victims' Rights Directive to ensure that victims of crime receive assistance, have access to information, can seek justice, and obtain compensation¹⁶.

However, the excessive fragmentation of European legislation, as well as the coexistence of different bilateral, trilateral and multilateral agreements, together with the cross-border nature of criminal activities, facilitated by the four fundamental freedoms provided for in Title V of the TFEU (Area of Freedom, Security and Justice), risk making all these instruments dangerously dysfunctional¹⁷.

Precisely for this reason, in December 2021 the EU approved a package of reforms, called the Police Cooperation Package, which is the expression of a precise and targeted strategy, aimed at strengthening cross-border police cooperation from an operational point of view. In fact, a Council Recommendation was adopted in June 2022 to strengthen operational cross-border police cooperation, which concerns joint patrols and police operations on the territory of another Member State; in May 2023 a Directive on the exchange of information between the police authorities of the Member States for the performance of activities other than those of the prevention and detection of criminal offences, which would remain governed, instead, by the Prüm II regulation, definitively adopted by the European Parliament in March 2024¹⁸, and applicable directly by the acceding Member States within a short period of its publication. The new regulation has been adopted in compliance with art. 16(2); 87(2)(a); 88(2) TFEU, and all Member States, including Ireland, participate in it, with the exception of Denmark, which, therefore, "is not bound by it or subject to its application"¹⁹.

While the Directive requires each State to introduce its own single point of contact, which should act as a point of contact to ensure the exchange and access to information, on equal terms, by police officers from all Member States, Prüm II has provided for an automated exchange of data for police cooperation. amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

In fact, Prüm II intends to further support national criminal investigations by adding to the automated exchange of DNA profiles, dactyloscopic data and vehicle registration data, also the automated search of digital facial images stored in national police databases, as well as giving Europol and its databases a strategic role.

On a structural level, the Regulation is divided into chapters and contains, first, the general provisions, indicating the subject, purpose and scope of application, followed by the provisions on automated exchange and consultation, as well as the types of "questions and answers" relating to the specific categories of data provided for by the Regulation. In more detail, these are DNA profiles, dactyloscopic data, vehicle registration data, facial images and extracts from the criminal record.

It also contains common provisions for the establishment of national contact points and the adoption of implementing measures. A central router is provided for and regulated for the exchange of data, and its use is regulated for the purpose of "launching" the various queries. Interoperability between the router and the common identity repository (for access by law enforcement authorities) is regulated, and it is also required, for the purpose of assurance, that a record of all data processing carried out remains.

Specifiche norme disciplinano l'uso dell'Indice europeo dei casellari giudiziari (EPRIS) a fini di scambio e, anche in questi casi, è prevista la registrazione di tutte le operazioni di trattamento: vengono definite le attività nel caso sia emersa una "corrispondenza" (hit).

Moreover, the automated exchange of basic data is limited to what is necessary for the identification of the data subject, while a more extensive exchange of data may be carried out at any further stage and for purposes other than mere identification.

There are provisions both on access by Member States to biometric data stored by Europol and from third countries, and on access by Europol to data stored in Member States' databases. Subsequently, when subjecting the data processed for the purposes of the Regulation to the provisions of Directive (EU) 2016/680 (LED), the prohibitions on the transfer and provision of data in an automated manner are expressly introduced, vis-à-vis third countries or international organizations. Supervision and auditing are also regulated to ensure adequate compliance with the rules described.

Infine, vengono individuate le competenze degli Stati membri, di Europol e di eu-LISA nell'attuazione dei contenuti del Regolamento, nonché le modifiche delle citate Decisioni 2008/615/GAI e 2008/616/GAI e dei Regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818.

Finally, the last chapter provides for some exceptions in the discipline, certain recognition and information obligations, including the preparation of reports and statistics, the making of notifications as well as transitional provisions. It also lays down the requirements for entry into force, as well as providing for the establishment of a committee and the adoption of a practical manual for the implementation of the Regulation.

To implement the provisions of the new regulation, a central router is also set up to simplify automated exchanges of biometric data, as well as a European Police Register Index System (EPRIS) to enable the automated exchange of police records.

Moreover, after a correspondence between the police of the Member States, confirmed on the biometric data through the exchange of identification data, it is provided that a follow-up within 48 hours is guaranteed.

It is, therefore, a reciprocal and automated exchange of data through a centralized system, to allow an easier, faster and more efficient exchange, thus representing a fundamental tool for law enforcement.

The router-based approach is hybrid, between decentralized and centralized, with no central data storage. Both the Prüm II and EPRIS central routers would serve as a connection point between the routers and the national databases of the Member States²⁰.

Therefore, cross-border criminal activities are, in essence, given a supranational response through greater coordination of the action of national police authorities, with the consequence that Security has become the new centre of gravity between the four European fundamental freedoms²¹. At the same time, we have moved from "justice" to "prevention", that is, from the search for a "legality of criminal justice" to a search for a "legality of security"²², in which procedural transparency between the various European bodies involved does not at all succeed in guaranteeing the other dimension of transparency, namely the technical one, which concerns the structural opacity of algorithms and artificial intelligence²³.

This finding is also confirmed, for example, by the power to report content "to the online service providers concerned for the purpose of voluntary examination of the compatibility of such content with their terms and conditions", introduced by Regulation (EU) 991/2022 reforming Europol²⁴, which, in turn, also seems to presuppose a proactive monitoring activity of Europol, to be carried out, probably, by means of artificial intelligence²⁵.

This paper will seek to demonstrate how the Prüm II Regulation, approved by the Council in February 2024, is not aligned with the safeguards provided by the LED, even limiting the protection of personal data and procedural rights, in contradiction with its own legal basis. Even more seriously, the regulation provides for restrictions on the right to the protection of personal data in violation of the principles of proportionality and necessity provided for in art. 8 of the Charter of Fundamental Rights of the European Union and art. 16(2) of the Treaty on the Functioning of the European Union (TFEU), according to which the restriction is lawful only taking into account the objectives of the measure itself and the need to protect rights and freedoms in general.

These profiles have given rise to a heated debate among scholars of social phenomena, to which have also been added case law that demonstrate how the Prüm II Regulation risks not being a fundamental opportunity to solve systemic problems in the cross-border exchange of data by law enforcement authorities²⁶.

Finally, the different solutions proposed by the literature will be analysed, the need for further changes to the new regulation, as well as possible future challenges in the field of data protection in the fight against national and cross-border crime.

2. THE ROLE OF EUROPOL

The European Police Office (Europol) was set up in 1992 with the aim of improving cooperation between the police forces of the Member States in the fight against terrorism, illicit drug trafficking and other serious forms of international organised crime but did not come into operation until 1998 based on the 1995 Europol Convention²⁷. Europol was subsequently governed by the Council Decision of 6 April 2009 (2009/371/JHA), and then by Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 (the so-called Europol Regulation), establishing the European Union Agency for Law Enforcement Cooperation (Europol), and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

The Europol Regulation aligns Europol with the requirements of the Lisbon Treaty, which entered into force at the end of 2009, as well as increasing its accountability by providing, *inter alia*, for the scrutiny of Europol's activities by the European Parliament and national parliaments. The new rules have enhanced the Agency's role as an information hub, reforming the methods of exchange with partners, strengthening the role of data management and protection with the creation of a new parliamentary control body, providing both the right of access to personal data,

and mechanisms for opposition and compensation for any unlawful management of the data themselves.

In fact, it is precisely the transnationality of organised crime, also driven by the data disseminated through the network, that has made collaboration between national and European authorities and EU agencies essential, i.e. automation and interconnection in the search for huge amounts of data available, as well as the usefulness in retrieval of information from private operators, which can often be identified in Internet Service Providers²⁸. The further progress and advancement of criminal groups, facilitated by the development of artificial intelligence, has made it necessary to use interoperable IT systems, specialized in the automatic control of the identity of non-EU citizens, crossing the external borders: European Border and Coast Guard Agency (FRONTEX), European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA), Schengen Information System (SIS) and European Travel Information and Authorisation System (ETIAS) which, in particular, will be operational from 2025. On the contrary, in June 2022 the new Regulation (EU) 991/2022 was approved with the aim of strengthening the interventions already carried out²⁹.

Probably, the reform aims to resolve an interinstitutional tension that has arisen between Europol and the European Data Protection Supervisor (EDPS), so much so that in December 2021 the EDPS signed a decision³⁰ by which EUROPOL was informed, pursuant to art. 18, paragraph 5 of the current Regulation, to delete within six months of receipt of the decision the data held by it, which had not been submitted to the Data Subjects Categorisation (DSC). In detail, the SDC consists of identifying, within these large databases, suspects, contacts and possible "associates", victims, witnesses and sources of information related to criminal activities.

The new Regulation 991/2022 and, above all, Article 18 thereof, will allow EUROPOL to operate through the processing of large and complex databases of personal data without the classification of data subjects (Data Subject Categorization, DSC) precisely for law enforcement purposes. Therefore, EUROPOL will also be able to process data relating to individuals, who are not related to the activities under investigation, whenever necessary to support the investigation.

On an operational level, in essence, the Regulation grants the Agency, subject to specific conditions, the possibility of also retaining data collected in previous years, for as long as and whenever it is required as an aid to an investigation, although a transitional regime has been put in place for information that has been processed by Europol before the amendments to the Regulation. In this way, the effectiveness of data processing without DSC is practically enhanced, expanding the amount of information to be cross-referenced³¹.

Also very important is the provision that the Agency will be able to receive data, i.e. electronic evidence, directly from those who hold them if they are deemed relevant for investigation purposes³². In addition, specific provisions provide for cooperation both for "online crisis situations" and cases of online dissemination of child sexual abuse material. While the former refers to "the dissemination of online content relating to an ongoing or recent real-world event that depicts harm to life or limb or that refers to imminent harm to life or limb and that has the object or effect of seriously intimidating the population, provided that there is a link or reasonable suspicion of a link to terrorism or violent extremism and that is expected to the exponential multiplication and virality of such content across various online services."

In addition, in order to further strengthen individual protection³³, but also Parliament's scrutiny and the Agency's accountability³⁴, Europol is granted the power to request the competent authorities of a Member State, even in the absence of the cross-border dimension of the offence,

in specific cases where it considers it appropriate to initiate a criminal investigation³⁵, to conduct or coordinate it, in case it affects a common interest of the Union³⁶.

Cooperation is also strengthened both internally, and with the EPPO, and externally, by strengthening collaboration with third countries for counter-terrorism purposes and with private individuals to obtain e-evidence. The proposal for a Europol reform ran parallel to the proposal for a reform of the Schengen Information System Regulation³⁷, under which Europol would be able to enter the SIS system data relating to suspected involvement of third-country nationals in an activity in which it is competent. The innovation of Europol's powers, in this way, has in some respects also overcome the impasse of the regulatory package on the order of production and storage of electronic evidence that has been discussed.

For the purposes of this analysis of the problems inherent in the Prüm regime, it should be borne in mind that it is precisely the new regulation that gives Europol a central role.

Europol's participation in the Prüm II regime allows Member States to verify biometric data shared with Europol by third countries, and Europol to verify the same data received from these third countries by comparing them with national databases. This system will facilitate criminal investigations by preventing gaps in crime and terrorism data received from third countries. However, some have also expressed concern that, like SIS, Europol is being used as a hub-like tool for laundering data received in breach of national law, as well as a conduit for harassing political opponents from third countries³⁸.

3. I ROUTER EUROPEAN POLICE RECORD INDEX SYSTEM (EPRIS) E PRÜM II

Europol is also tasked to develop and maintain EPRIS (European Police Record Index System), which forms the technical basis for the exchange of police records³⁹.

Indeed, Prüm II Regulation No 982/2024 provides that to speed up access to data for cross-border cases under criminal investigation, two central routers will have to be created, the Prüm II router and the European Criminal Records Indexing System (EPRIS).

Section 2 of Articles 42 to 46 regulates EPRIS, which is used by Member States and Europol for the automated search of criminal records⁴⁰.

EPRIS consists of a central infrastructure, including a search tool that allows simultaneous querying of Member States' databases, as well as a secure communication channel between the EPRIS central infrastructure, the Member States and Europol.

For the consultation of criminal records through EPRIS, then, the data relating to the name(s), surname(s) and date of birth are used. However, if available, other data may also be used, such as alias, nationality or nationality, place and country of birth, gender. In addition, almost all the data used for queries is pseudonymised.

Organisationally, the Member States and Europol request a search by submitting such data, while EPRIS sends such a request for a query to the Member States' databases, which initiate a search of their national police records archive in an automated manner and without delay. All matches resulting from the search in each Member State's database are then automatically returned to EPRIS, which then returns them to the requesting Member State.

Subsequently, the requesting Member State decides which matches for which follow-up is required and, accordingly, sends to the requested Member State(s) via Secure Information Exchange Network Application (SIENA)⁴¹ a reasoned follow-up request containing all additional relevant information.

Both Europol and each Member State shall keep records, as well as related data, of all data processing operations in EPRIS carried out by its duly authorised staff.

Such records may only be used for data protection monitoring, including verifying the admissibility of a query and the lawfulness of data processing, and to ensure data security and integrity. In addition, these registers shall be protected by appropriate measures against unauthorised access and deleted one year after they are created.

On the other hand, if they are necessary for monitoring that has already begun, they will be deleted once the monitoring procedures no longer require registrations.

As far as the Prüm router is concerned, it would allow Europol access to databases held by EU countries, and vice versa, to automatically check biometric data from third countries.

Finally, pursuant to Regulation (EU) 2018/1725, the controller of personal data via the router is eu-LISA, while Europol is the controller of personal data through EPRIS. Both will then have to adopt specific security and monitoring measures for the processing of data provided for by the regulation and cooperate in all types of checks set up by the European Data Protection Supervisor, including every four years.

4. WHAT ARE THE CHALLENGES OF PROTECTING PERSONAL DATA IN PRÜM II AND EPRIS?

The data protection system embedded within the citizens' security system, as provided for by the Prüm II Regulation, adopted by the European Parliament and Council in March 2024, has many critical aspects, which can undermine the protection of data itself.

On the one hand, Prüm II increases the automation of data sharing; adds new categories of data that can be shared, such as facial images, criminal records and driving licence data; standardizes the format in which data can be shared, thus facilitating future integration with other systems; sets new standards on data quality, transfers and other largely technical elements; Finally, it creates a legal basis for searches for missing persons and unidentified human remains.

On the other hand, however, Regulation (EU) 2024/982 does not establish, for example, legal thresholds to limit data sharing, such as the seriousness of the crime, of which, however, Europol only provides a generic definition, without specific details.

An in-depth analysis of the legislative text reveals an intrinsic contradiction of the rules. Indeed, although the Prüm II proposal falls within the scope of the LED⁴², in practice it is difficult to achieve a coherent data protection regime for all EU police and criminal justice measures. It may be difficult, for example, to represent Prüm's specific purpose limitation requirements in the general data protection rules applicable throughout the industry. In particular Article 26 of Council Decision 2008/615/JHA on purpose limitation, which was not deleted by Regulation No 982/2024, distinguishes between two situations. First, the processing of personal data by the receiving Member State is permitted, generally, only for the purposes of the decision or, exceptionally, with the prior consent of the Member States concerned⁴³. In practice, it is a

question of preventing crime and maintaining public order and security at major events⁴⁴. Secondly, and more specifically, the processing of data by automated search or comparison of DNA profiles or dactyloscopic data is permitted only in specific circumstances, i.e. to determine whether DNA profiles or dactyloscopic data match; to prepare a police or judicial request for legal assistance if the data match, and to perform logs and recordings⁴⁵. On the contrary, the LED provides for the possibility of processing personal data "*for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [...]*"⁴⁶. It therefore remains very general and does not take into account the specificities of the Prüm regime, in particular as regards the automated nature of the transactions.

It can also be observed that even after the adoption of Regulation (EU) 2024/982, there continue to be several fragmentations between EU Member States in the criteria for the retention and inclusion of forensic database data, in addition to the inclusion and preservation of profiles of children and innocent people in forensic DNA databases⁴⁷. For example, while Sweden only includes personal data in the DNA database if the person has been found guilty of a crime and sentenced for more than two years, the Netherlands adds any person who has committed a crime, except where the penalty consists only of paying a fine⁴⁸. This is just one example of the overall fragmentation of existing national rules, which raises legitimate concerns, as some Member States may process and store personal data, which in principle should not be legally present in their systems. In this complex context, there is also the different data protection regime applicable to Europol, whereby there is a lack of coordination between legal frameworks and regimes, which also calls into question the need for many of the profiles including numerous national databases⁴⁹. From a practical point of view, for example, a person could be included in a database in one Member State participating in Prüm II, and excluded in another, creating a mosaic of names with different protections.

Even the conditions for justifying a search, i.e. a 'query', of a database differ from one Member State to another.

These aspects are not adequately addressed by the Prüm II regime, with the result that persons registered in a police database in a Member State, where there are lower thresholds for inclusion and less effective surveillance mechanisms, will be more likely to be subject to potentially unjustified 'police attention' than persons benefiting from standards⁵⁰. Forsooth, these people will be unfairly subject to the simultaneous increased risk of violations of their rights to due process, to effective remedy, as well as to privacy and data protection⁵¹.

While the fight against organised crime, both national and cross-border, is undoubtedly a legitimate and important objective, it is also understood that this is achieved in such a way as to prevent arbitrary intrusion into the rights of individuals, as well as to respect the right of individuals both to the presumption of innocence and to a fair trial, in which the admission of evidence in court is guaranteed.

These ethical principles applicable to law, however, are not always respected. In fact, a police report based on data from the European Network Against Racism (ENAR) shows that many law enforcement databases across Europe, containing biographical information, as well as biometric and other sensitive personal data, often have dangerous inaccuracies, biases and examples of potentially illegal profiling⁵², as is also represented by the graph below (Figure 1).

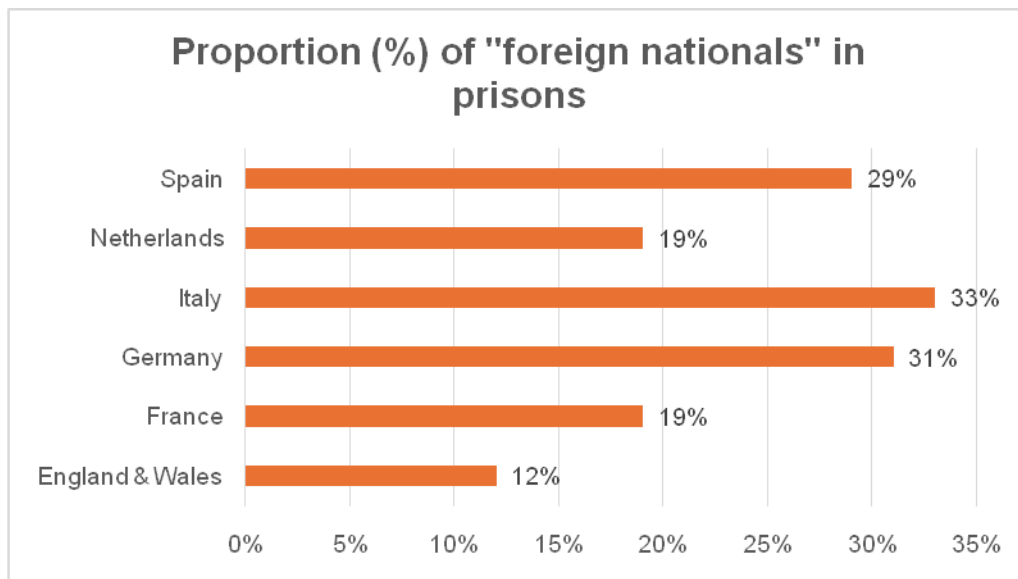


Figure 1. Source: Aebi, M.F. et al (2018) 'Foreign offenders in prison and probation in Europe: Trends from 2005 to 2015 (inmates) and situation in 2015 (inmates and probationers)'. University of Lausanne: Council of Europe.

For example, in the Netherlands, people are included in pseudo-criminal biometric databases only for the "crime" of being a foreigner, or they are unduly included in criminal databases without a legal basis and without the possibility of redress or removal⁵³. In other European countries, these kinds of databases are used politically for repressive use, such as in Austria, where police added about 640,000 entries to the new facial database in a year, including those of protesters, who are far from the serious criminals for whom the system was intended⁵⁴.

Unfortunately, these are not isolated cases, or computer errors, but the inability to process police data in accordance with the safeguards provided by the LED. This observation is also confirmed by the European Union Agency for Fundamental Rights (FRA) which, in 2021, confirmed that across Europe "Blacks, Asians and Roma are even more likely to be stopped and searched by the police"⁵⁵. In particular, the Agency explained that "persons belonging to ethnic minorities" are more than twice as likely to be questioned for their identity, while they are half as likely to perceive that they have been treated with respect by the police during such stops⁵⁶. It can be observed that these biases and acts of profiling will inevitably be reflected in the data collected and coded in databases, thus consolidating and perpetuating discrimination.

The gravity of these facts is also accentuated by Freedom House, which in 2022 presented the Rule of Law Report, according to which in several EU countries, including France, the Netherlands, Cyprus, Portugal, Poland, Lithuania and Latvia, society would become "less free" between 2020 and 2021, highlighting how many democratic standards have been eroded in several EU countries⁵⁷.

In the current Prüm regime, the European Commission has also observed an initial crisis of the rule of law in Europe⁵⁸, often characterized by racism and control of minorities, the increasing criminalization of political opposition, refugees, migrants, as well as those acting in solidarity with them by providing humanitarian aid, as well as investigative journalists.

In recent years, for example, the European Commission has imposed sanctions on Hungary and Poland because of proceedings finding violations of the rule of law and threats to the

independence of the judiciary. In addition, systemic deficiencies in the functioning of national police databases have been documented across Europe⁵⁹.

The rule of law review mechanism has also been criticised by the European Parliament, as well as by independent evaluations⁶⁰.

Abuses of data processing were also found by Europol when, in both 2020 and 2022, the EDPS admonished the Agency and ordered the deletion of illegally processed and stored data due to systematic deficiencies, which had led to the Agency's own examination of large volumes of data in a way that violated fundamental rights⁶¹.

Europol's collection of biometric data is also a matter of great concern. Many believe that Member States should adopt, for the protection of individuals, clear rules for the collection and storage of biometric data by authorities, for example, by preventing the indefinite retention of biometric data of persons simply accused of a crime⁶². The need for such measures would also be confirmed by the fact that Europol can receive biometric data from third countries based on rather general criteria, already provided for in the 2022 Europol Regulation, and there is no absolute certainty that these refer only to terrorists, convicted persons, suspected terrorists and other serious criminals⁶³.

There are also studies that show that the available data on DNA exchange show a "little usefulness" of the system to obtain information after a confirmed "positive finding" and that, much more seriously, some innocent people have been falsely arrested because of poor quality DNA matches through the Prüm framework⁶⁴.

Moreover, the small amount of data that society is able to analyse does not demonstrate any statistically significant correlation between the number of DNA searches carried out by Member States in 2021, through the Prüm framework, and the number of matches to which those searches led⁶⁵. In particular, the high number of searches carried out in Austria and Germany did not lead to a statistically significant increase in matches, casting doubt on the very premises of Prüm II⁶⁶.

Also, with reference to the processing of data for the identification of missing persons, or the identification of unknown remains, it can be observed that there is no absolute certainty as to whether these can always, in all cases, have links with serious cross-border crimes. The indiscriminate inclusion of 'missing persons and unidentified human remains' (Article 2) in the Prüm II Regulation would therefore lack a specific legal basis, leading to possible abuses and excesses, not least because the EU's SIS II system already allows missing persons to be flagged based on fingerprints and even DNA⁶⁷.

There are many alleged LED violations. From a procedural point of view, for example, the requested Member State does not have the possibility to assess in advance the necessity, or proportionality, of a search, or the accuracy of the data retained, before the publication of the biometric profile. Also, since profiles are always returned in the form of a list of potential matches (1st most likely match, 2nd most likely match, etc.) (Article 37.5), this means that even the sensitive biometric profiles of people who do not match, but are still on the list, will always be automatically shared for the purpose of making a comparison⁶⁸.

Well-founded concerns have also been raised regarding the facial recognition system, due to the significant number of errors recorded in the correct identification of individuals.

In fact, the episodes of racial discrimination inherent in the results guaranteed by these algorithms are well known, which, for example, in the United States have considerably higher margins of

error in the identification of African American subjects rather than Eurasian ones, due not to computational errors, but to cultural and cognitive factors of society.

Therefore, the positions of those who, while waiting for a refinement of facial recognition mechanisms, call for their use to be limited only for the fight against the most serious crimes, the identification of which should be done upstream by the legislator⁶⁹, and with a view to a balance between the needs of security and freedom of citizens, seem to be shared.

The criticisms that have already been made so far would entail serious risks for fundamental rights, such as weakening the presumption of innocence, enabling mass surveillance, criminalising migration through expansion to other categories of data, exacerbating trends such as systemic discrimination in the police force, and the wider crisis of the rule of law in Europe⁷⁰ as well as reducing the control "that citizens have over law enforcement and creeping police surveillance"⁷¹.

Da una lettura attenta del regolamento Prüm II emerge, poi, che agli Stati membri aderenti non viene previsto un diritto di rifiuto prima dello scambio di dati personali, magari per valutare semplicemente se si tratta di casi realmente individuali e solo in caso di crimini gravi, ma solamente il diritto di accesso alle giustificazioni per il trattamento dei dati (articolo 33)⁷².

In contrast to the above, authoritative opinions have expressed themselves in favour of the new regulation, arguing that it is precisely the automated exchange of data for police cooperation that will make it possible to combat both organised crime and terrorism effectively and on a daily basis, despite these concerns, because national law enforcement agencies will be able to know more efficiently and quickly whether other Member States or Europol have data related to an ongoing criminal investigation⁷³, always limited to the prevention, detection or investigation of criminal offences. Prüm's framework has proved instrumental in solving many crimes in Europe⁷⁴, such as in the Italian case of the murder of Yara Gambirasio in which judicial investigations were based almost exclusively on DNA profiles; this legislation will be greatly improved by adding facial images of the faces of suspects and criminals already convicted by the police. as well as data centralization. In addition, in accordance with the fundamental freedoms, a specific rectification procedure is provided for in the event of inaccurate data, and for the immediate deletion of the data at the end of the automated response to the consultations, unless further processing is required for registration in accordance with Article 51 of the Regulation. In particular, the new Prüm II Regulation will close previous information gaps and promote security for all in Europe also through the involvement of Europol and searches on vehicle registration data using criminals' identity data⁷⁵.

In conclusion, however, even if those assertions were to be accepted, it remains to be observed that the Prüm II Regulation allows for the perpetual automated search of all unidentified DNA profiles in relation to all other DNA profiles in the framework. It is, therefore, an automated mass search, which inverts and violates the principle of the presumption of innocence, as well as being disproportionate, by configuring forms of mass biometric surveillance⁷⁶, which also include facial images subjected to specific technical processing, like Bentham's Panoptic.

5. CONCLUSIONS AND POSSIBLE FUTURE DEVELOPMENTS

The Prüm II regime, analyzed above, tends to emphasize security measures, which treat individuals as potential criminals, rather than addressing the underlying causes of crime and prioritizing less intrusive alternatives. Moreover, this is taking place within a very fragmented regulatory system on the protection of data for individuals, which will make it more difficult for data subjects to defend their rights.

Whereas the Court of Justice has already ruled, in the well-known *Tele2 Sverige* case of 2016, in relation to the disproportionate nature of the general and indiscriminate retention of traffic and location data⁷⁷, has clearly distinguished between the processing of data for the purpose of preventing serious crimes and the prevention of minor crimes or the efficient management of non-criminal proceedings, it can be expected that the inclusion of facial images, as well as a low threshold for offences in the Prüm II rules, will increase legal disputes in court in the near future⁷⁸.

These existing challenges and fragmentation will be further exacerbated, with the adoption of Prüm II and the Artificial Intelligence Act. New specific legal frameworks on data protection will add to the complex patchwork of legal instruments that already exist, making it even more complicated for data subjects to defend their rights.

However, there can also be no doubt that the coordinated combination of the Prüm II legal system, the EPRIS platform and the recent approval of the European Artificial Intelligence Regulation will⁷⁹ strengthen the police's ability to find missing and unidentified persons in the EU, as well as to identify unidentified human remains quickly and consistently.

In fact, the prediction is of paramount importance, especially considering that more than 300,000 people disappear every year in Europe, according to data from 18 EU countries, of which only a small proportion (1-4%) of these cases are linked to criminal activities⁸⁰.

In particular, the data collected show that since 2018 almost 17 migrant children have disappeared in Europe every day⁸¹. We must not forget that the European Court of Human Rights has established the primary obligation of law enforcement agencies to protect life itself.

In conclusion, without the necessary substantive revisions, the Prüm II Regulation could be annulled by the CJEU, jeopardizing its stated objective of fighting crime in compliance with EU law.

REFERENCES

- [1] United Nations, United Nations Convention against Transnational Organized Crime and the Protocols Thereto, 2000, on <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html#Fulltext> .
- [2] EUROPOL, Definition of serious and organised crime, in <https://www.europol.europa.eu/socta/2017/defining-serious-and-organised-crime.html> .
- [3] Published in OJEU, C 53, 3 March 2005, p. 1.
- [4] Angela Procaccino, *Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione, Diritto Penale Contemporaneo, Rivista trimestrale, 1/2023, p. 145 ss.* In fact, Directive (EU) 2016/680 of the European Parliament and of the Council of Europe, guarantees the protection of the personal data of persons involved in criminal proceedings, whether they are witnesses, victims or suspects, by harmonizing the rules applicable in the Member States of the European Union and in the Schengen countries. This regulatory instrument is part of the data protection reform, together with the GDPR and Regulation (EU) 2018/1725 on the protection of natural persons regarding the processing of personal data by the Union institutions, bodies, offices and agencies.
- [5] EDRI, *Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRI) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")*, 7 September 2022, in <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>.
- [6] European Council, Council of the European Union, *The EU's fight against organised crime*, in <https://www.consilium.europa.eu/it/policies/eu-fight-against-crime/#priorities> .
- [7] Commissione Europea, *Strengthening the automated data exchange under the Prüm framework*, in https://home-affairs.ec.europa.eu/whats-new/strengthening-automated-data-exchange-under-prum-framework_en . L'Europol è l'agenzia di contrasto dell'UE che assiste i 28 Stati membri dell'UE nella lotta contro le forme gravi di criminalità internazionale e il terrorismo.
- [8] See previous note.
- [9] In fact, the instrument in question does not have a specific and autonomous legal basis since it is likely to fall within the general competences of the Council of the European Union. In any case, the presentation, structure and details of the competences contained in the plan are contained in the Annex, called Terms of References to a Note of the Presidency of the Council of Ministers to the Delegates of 17 June 2021, no. 9921/21, available at the website www.data.consilium.europa.eu.
- [10] Assai interessante notare come proprio nell'apertura dei "Terms of Reference", citati alla nota precedente, si affermi come uno dei punti chiave di EMPACT sia: "(T)the intelligence-led approach based on a future-oriented and targeted approach to crime control, focusing upon the identification, analysis and "management" of persistent and developing "problems" or "risks" of crime".
- [11] In fact, on 16 September 2020, the President of the European Commission announced, in the letter of intent that accompanied the "State of the Union" Report addressed to the European Parliament, a new agenda on organized crime, which is part of the so-called New Security Union Strategy, i.e. a "broader action" in Security.
- [12] See: Letter of intent: Key New Initiatives for 2021, del settembre 2020; Communication on the EU Security Union Strategy, COM(2020) 605 final; Fighting organised crime – EU strategy for 2021-25; European Union Serious and Organised Crime Threat Assessment (EU SOCTA 2021); Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions on the EU Strategy to tackle Organised Crime 2021-2025, COM/2021/170 final.
- [13] Angela Procaccino, *Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione, Diritto Penale Contemporaneo, Rivista trimestrale, 1/2023, p. 145 ss.*
- [14] See previous note.
- [15] European Council, Council of the European Union, *The EU's fight against organised crime*, in <https://www.consilium.europa.eu/it/policies/eu-fight-against-crime/#priorities> .
- [16] See previous note.
- [17] See the Assessments contained in the preamble to the Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ('Prüm II'),

- amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) 2019/817 and (EU) 2019/818, resulting from the closure of the public consultation procedure, can be found at the site www.ec.europa.eu, 3, p. 6.
- [18] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on automated consultation and data exchange for police cooperation and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (Prüm II Regulation), on <https://eur-lex.europa.eu/eli/reg/2024/982/oj>.
- [19] See previous note.
- [20] Gert Vermeulen, (2021), EU Criminal Justice and Law Enforcement Cooperation: Never a Dull Moment, in RIDP, Wannes Bellaert, Gert Vermeulen, (Eds.), EU Criminal Policy: Advances and Challenges, Volume 92 issue, 2, p. 16 e ss.
- [21] Angela Procaccino, (2023) *Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione, Diritto Penale Contemporaneo, Rivista trimestrale, Vol.1, p. 145 ss.*
- [22] See previous note.
- [23] See Quattrococo, Serena (2018): "Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienza penali e informatiche", www.lalegislazionepenale.eu.
- [24] Regolamento (UE) 991/2022, entrato in vigore il 28 giugno 2022.
- [25] Angela Procaccino, (2023), *Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione, op. cit.*
- [26] EDRI, *Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")*, op. cit.
- [27] See https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/europol_it.
- [28] For an explanation of the changed criminal and technological context, see Recitals 1, 2, 3 and 6 of Regulation (EU) 991/2022 reforming Europol. For the "manifesto" of the Regulation and the reference to the rootedness in art. 4(2) TEU, for the purpose of protecting the national security of the Member States, cf. recitals 4 and 5, also with a view to strengthening the Interoperable Special Intervention Units (referred to in the above-mentioned Council Decision 2008/617/JHA of 23 June 2008 on improving cooperation between the Special Intervention Units of the Member States of the European Union in crisis situations).
- [29] See, in fact, recital 8 of the EUROPOL Reform Regulation (EU) 991/2022, which states that "Europol should be able to facilitate and support intelligence-based security initiatives launched by Member States — such as the European Multidisciplinary Platform against Criminal Threats (EMPACT) — aimed at identifying, prioritising and addressing serious crime threats. Europol should be able to provide administrative, logistical, financial and operational support to such initiatives."
- [30] The "Decision on the retention by Europol of datasets lacking Data Subject Categorisation", taken pursuant to art. 43(3) of the EUROPOL Regulation, which defines the powers of the EDPS, including the power to order the possible deletion of data stored and retained in breach of EUROPOL legislation.
- [31] This aspect is also deeply linked to the other relevant innovation relating to research and development activities in the field of artificial intelligence: in fact, a legal basis dedicated to the processing of personal data for research and innovation purposes is introduced, accompanied by data protection guarantees (e.g. pseudonymization), which will be applicable to such processing (see art. 2, letters v), and 4, paragraph 1, letters v) and w), Regulation 991/2022). These provisions constitute the legal basis for the use of Artificial Intelligence by EUROPOL, which can most likely also be used for "predictive policing" purposes.
- [32] The rules on "Relations with Partners" are contained in Chapter V of the Regulation, in art. 23 ff. See art. 26, 26-bis and 26-ter for the exchange of personal data with "private parties". Art. Article 27 regulates "(D)information from private persons".
- [33] An independent office, the Fundamental Right Officer (FRO), has been set up to work alongside the independent Data Protection Officer (DPO), who already exists in Europol's organisation. It should

also be noted that, even though since 1 May 2017, the EDPS had competence to supervise the processing of personal data by Europol, the reform of the Regulation has provided for a strengthening of the supervisory functions of the same.

- [34] It is worth noting that the corrections relating to the reinforcement of protection in the data processing process are due to the opinion of the European Data Protection Supervisor (EDPS) issued on 8 March 2021 in which it was recommended, among other things, that certain concepts in the proposed Regulation be better defined; that safeguards relating to derogations from the processing of large data sets should be strengthened; It also recommended that massive and structural transfers with all private individuals in the EU be prohibited. On the other hand, the European Economic and Social Committee (EESC), in its opinion of 9 June 2021 (available at www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/strengthening-europols-mandate), did not express concerns about the proposed regulation on the points in question, but instead welcomed the increase in Europol's budget to further protect EU citizens. See EDPS Opinion on the Proposal for Amendment of the Europol Regulation, available at www.edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf.
- [35] These are genuine own-initiative investigations. Of course, with some limitations: that is, it is up to the Executive Director of Europol to propose the opening of a national investigation into a specific crime that affects only one Member State but harms a common interest covered by a Union policy. However, it will be up to the national authorities to assess the proposal.
- [36] The European Economic and Social Committee (EESC) in the opinion cited in the previous note, in positively evaluating the proposed Regulation, even suggested that the time had come "to allow Europol to act on its own initiative".
- [37] Regulation (EU) 2018/1862 on the Schengen Information System, on the structure of which and on whose interrelations with EUROPOL. See, Gialuz, Mitja (2022): "Horizontal cooperation", in Kostoris, Roberto (editor), *Manual of European Criminal Procedure* (Milan, Giuffrè), pp. 313 ff.
- [38] Jane Kilpatrick and Chris Jones, (2022), 'Empowering the Police, Removing Protections: The New Europol Regulation', Statewatch, on <https://www.statewatch.org/media/3615/empowering-the-police-removing-protections-new-europol-regulation.pdf>.
- [39] See <https://www.statewatch.org/media/documents/analyses/no-145-ecris-epris-ixp.pdf>
file:///C:/Users/39339/Downloads/study%20on%20possible%20ways%20to%20enhance%20efficiency%20in%20the-DR0113048ENN.pdf
- [40] See https://www.eumonitor.eu/9353000/1/j4nvhdsc8bljza_j9vvik7m1c3gyxp/vlolhyw3zyzw
- [41] Lake <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena>.
- [42] Directive 2016/680 on the protection of personal data with regard to the processing of data by police and criminal justice authorities (the "Law Enforcement Directive", LED).
- [43] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008 (OJ 2008 L) Article 26(1).
- [44] See previous note, 14.
- [45] See previous note, 26(2).
- [46] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Article 1(1).
- [47] Filipe Santos, Helena Machado and Susana Silva, (2013), "DNA Forensic Databases in European Countries: Is Size Related to Performance?", 9 *Life Sciences, Society and Politics* 12.
- [48] EDRI, (2022), 'Respect for fundamental rights in cross-border investigations of serious crime - EDRI Network Position Paper on Automated Data Exchange for Police Cooperation ('Prüm II')', 8.
- [49] EDRI, (2022), 'Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRI) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")', op. cit.
- [50] See previous note.
- [51] See previous note.
- [52] ENAR, (2019), *Data-Driven Policing: The Hardwiring of Discriminatory Police Practices across Europe*, available at: <https://www.statewatch.org/media/documents/news/2019/nov/data-driven>

- profiling-web-final.pdf; In fact, people are "systematically overrepresented" in police databases across Europe according to the Equinox Racial Justice Initiative. See <https://www.equinox-eu.com/wp-content/uploads/2021/10/Equinox-Who-Protects-Us-from-the-Police.pdf>. In addition, the UK's "Gangs Matrix", for example, has also been criticised for unfairly targeting young people of colour and other people belonging to minorities. See <https://www.independent.co.uk/news/uk/home-news/met-police-gangs-matrix-database-b2004293.html>. In addition, there is evidence that people who are victims of racism are vastly overrepresented in the country's criminal justice system in general. In this sense, see 'Ethnicity and the criminal justice system: What does recent data say on over-representation?', House of Commons Library, 2, October 2020, <https://commonslibrary.parliament.uk/ethnicity-and-the-criminal-justice-system-what-does-recent-datasay>. The Netherlands' 'Top400' and 'Top600' databases have also received similar criticism from criminal justice watchdog Fair Trials for illegitimately targeting young people from poor and minority backgrounds, automating the injustice they face at the hands of the state. To this effect, see https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.
- [53] New EDRI report reveals depths of biometric mass surveillance in Germany, the Netherlands and Poland, in <https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/>.
- [54] EURACTIV, Austrian facial recognition database collects over 600,000 entries in a year, in https://www.euractiv.com/section/politics/short_news/austrian-facial-recognition-database-collects-over-600000-entries-in-a-year/.
- [55] FRA, (2021), European Union Agency for Fundamental Rights, Police stops in Europe: everyone has a right to equal treatment, in <https://fra.europa.eu/en/news/2021/police-stops-europe-everyone-has-right-equal-treatment>.
- [56] See previous note.
- [57] Freedom House, Change in Freedom Score From 2022 to 2023, in <https://freedomhouse.org/explore-the-map?type=fiw&year=2022&mapview=trend>.
- [58] European Commission, 2022 Rule of law report - Communication and country chapters, July 2022, in https://commission.europa.eu/publications/2022-rule-law-report-communication-and-country-chapters_en.
- [59] ENAR, (2019), Data-driven policing: the hardwiring of discriminatory policing practices across europe,
- [60] European Parliament, News, Rule of law in the EU: ways to better protect the Union's core values, 2022, in <https://www.europarl.europa.eu/news/en/press-room/20220620IPR33409/rule-of-law-in-the-eu-ways-to-better-protect-the-union-s-core-values>.
- [61] See https://www.edps.europa.eu/system/files/2022-08/2022-04-20-edps-annual-report-2021-executive-summary_it.pdf.
- [62] European Court of Human Rights, judgment in the case of S and Marper v United Kingdom, para. 125, <https://hudoc.echr.coe.int/eng?i=001-90051>.
- [63] Europaen Data Protection Supervisor, Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prum II"), 2022, in https://www.edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf.
- [64] European Parliament, Study For the LIBE committee, Cross-border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision, Policy Department for Citizens' Rights and Constitutional Affairs, (June 2018), in [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU\(2018\)604971_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf).
- [65] Analysis based on <https://www.statewatch.org/media/3248/eu-council-prum-statistics-2021-5436-22.pdf> and available on request.
- [66] See previous note.
- [67] EDRI, Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRI) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II"), op. cit.
- [68] See previous note.
- [69] See previous note.
- [70] See previous note.
- [71] See <https://pirati.io/2024/02/condivisione-dei-dati-della-polizia-prum-ii-manca-di-garanzie/>,

- <https://www.irpa.eu/il-prum-ii-lautomatizzazione-dellattivita-di-polizia-tra-sicurezza-e-privacy/> .
- [72] See <https://edri.org/our-work/new-eu-law-amplifies-risks-of-state-over-reach-and-mass-surveillance/> , <https://eucrim.eu/news/civil-rights-organisations-criticise-prum-ii-proposal/> .
- [73] See <https://www.consilium.europa.eu/it/press/press-releases/2023/11/20/council-and-eu-parliament-reach-deal-to-advance-police-cooperation-in-europe/> .
- [74] Si veda https://enfsi.eu/wp-content/uploads/2016/09/enfsi_report_on_criminal_cases_in_europe_solved_by_ils_0.pdf
- [75] See previous note.
- [76] See, for example, <https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>.
- [77] Court of Justice, Grand Chamber, 21 December 2016, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB (C-203/15).
- [78] EDRI, (2024), Automated data exchange in Prüm II: The EU’s securitisation mindset keeps encroaching on our fundamental rights, in <https://edri.org/our-work/automated-data-exchange-in-prum-ii-eu-securitisation-mindset-encroaching-on-fundamental-rights/> .
- [79] See <https://www.europarl.europa.eu/news/it/press-room/20240308IPR19015/il-parlamento-europeo-approva-la-legge-sull-intelligenza-artificiale> .
- [80] European Centre for Missing Children, (2023), Call to european parliament: vote in favour of keeping the search of 40,000 unresolved missing persons cases and 15,000 unidentified human remains in the prüm ii framework, on <https://www.amberalert.eu/news/call-to-ep-vote-prum-ii> .
- [81] The Guardian, (2018), Nearly 17 child migrants a day vanished in Europe since 2018, Investigation finds one in six were solo and under 15, as experts say cross-border cooperation ‘nonexistent’, on <https://www.theguardian.com/global-development/2021/apr/21/nearly-17-child-migrants-a-day-vanished-in-europe-since-2018> .

AUTHOR

Cavalli Ramona, Researcher at the Department of Demography and Social Statistics of the Italian National Institute of Statistics in Rome. Adjunct Professor at the University of Verona, Italy. Ph.D. in Public Economic Law. Lawyer. Author of numerous publications on privacy and social research.