European security governance: Europol's oversight in the era of Big Data and Automated Decision-Making

Jaseff Raziel Yauri-Miranda
Erasmus University Rotterdam & University of the Basque Country

Abstract:

This study critically examines the accountability mechanisms within Europol, focusing on key legislative frameworks such as the Europol Regulation (2016/794), the GDPR, and Regulation (EU) 2018/1725. The study assesses Europol's regulation for data exchanges, the role of the European Data Protection Supervisor (EDPS), and the challenges of ensuring effective oversight amidst technical and operational complexities. How effective are the current accountability mechanisms at Europol, particularly in the context of big data and automated decision-making, and what improvements can be made to enhance accountability beyond risk assessment and data protection standards? The study explores the challenges of automated decision-making, emphasizing issues like automation bias and the limitations of human oversight. It analyzes Europol's accountability structures, particularly in data protection and the risks associated with external informational infrastructures. The study concludes by claiming for a more robust accountability governance framework integrating risk assessment, internal operations, and external oversight.

Keywords: Accountability, Europol, Big Data, Automated Decision-Making, Data Protection

Introduction

Europol's origins can be traced back to the Maastricht Treaty negotiations in 1992, where the concept of a European police office was first proposed. In 1995, Europol began its initial operations as the Europol Drugs Unit (EDU), focusing primarily on combating drug-related crime. The Europol Convention, ratified by all EU Member States in 1998, expanded the agency's mandate to tackle a broader range of serious international crimes (Bruggeman, 2002). Officially launched as a fully-fledged European law enforcement agency in 1999, Europol established its headquarters in The Hague, Netherlands. In the early 2000s, Europol's mandate grew to include all forms of serious international crime, such as terrorism, human trafficking, and cybercrime. The Europol Council Decision in 2009 replaced the Europol Convention, simplifying the legal framework and funding Europol directly from the EU budget (Busuioc & Groenleer, 2016). This decision further integrated Europol into the EU's institutional framework, significantly enhancing its capabilities and scope.

To enhance accountability, the Joint Parliamentary Scrutiny Group (JPSG) was created under Article 51 of the Europol Regulation (Decision - 2009/371)[1], allowing for increased oversight by the European Parliament and national parliaments. This mechanism ensures political scrutiny of Europol's activities, enhancing transparency and oversight. Transparency provisions were further strengthened by requiring the publication of Management Board summaries and applying Regulation (EC) No 1049/2001 to provide public access to Europol documents.[2] Furthermore, the introduction of the Europol Regulation in 2017 marked a significant milestone, providing a clearer legal basis for Europol's operations and enhancing its role in combating terrorism and cybercrime.[3] This regulation also bolstered data protection measures, introducing the appointment

[1] Europol Decision - 2009/371, Council Decision of 6 April 2009 establishing the European Police Office (Europol), available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009D0371

[2] Regulation (EC) No 1049/2001 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049

[3] Article 65 of the Europol Regulation by the Management Board on 13 December 2016 became applicable as of 1 May 2017, consult https://www.europol.europa.eu/publications-events/public-access-to-europol-documents

of a Data Protection Officer (DPO) and oversight by the European Data Protection Supervisor (EDPS). National supervisory authorities were designated by Member States to oversee data transfers and compliance with national laws and the Cooperation Board, comprising representatives from these national authorities and the EDPS, was established to ensure harmonized supervision across the EU.[4]

The accountability of Europol, the European Union Agency for Law Enforcement Cooperation, is part of an intricate governance and essential aspect of its operational mandate. As Europol serves a crucial role in facilitating cooperation among EU member states to combat serious international crime and terrorism, it is imperative that its activities are conducted transparently and within the bounds of the law. However, ensuring this requires a robust framework of oversight and accountability, designed to uphold public trust and safeguard the rights of individuals is not straightforward.[5] This paper provides a comprehensive analysis of the current legislative and policy structures underpinning Europol's accountability, scrutinizing the effectiveness and challenges of these mechanisms. In the light of that, the central research question guiding this investigation is *How effective are the current accountability mechanisms at Europol, particularly in the context of big data and automated decision-making, and what improvements can be made to enhance accountability beyond risk assessment and data protection standards?* This question aims to explore the adequacy of existing regulatory frameworks and oversight practices, identifying gaps and challenges, and proposing some recommendations for strengthening Europol's accountability in handling large datasets and automated processes.

The paper is structured as follows: Part 1 draws from the legislative Europol Regulation, showing a comprehensive legal instrument that delineates the agency's mandate, operational scope, and governance structures. This regulation outlines critical aspects of Europol's accountability framework, including the roles and responsibilities of various oversight bodies, data protection standards, and risk management practices. Part 2 explores one of the core fronts for Europol's accountability: data protection rules established through key provisions in the last years. Central to this framework, the study analyzes the role of the European Data Protection Supervisor (EDPS), highlighting significant instances where the EDPS has influenced Europol's data protection practices, such as opinions on several high-profile projects, which required Europol to make significant adjustments to ensure compliance.

Part 3 analyses Europol's governance dimensions and risk management policy. Introduced in 2022, this policy defines risk as any uncertain event that could impact the achievement of objectives related to annual business planning and the Europol Strategy 2020+. This part also explore human intervention governance in automated decision-making (ADM) systems as these also presents significant accountability challenges, highlighting the importance of balancing efficiency with contextual governance considerations, especially in relation to the deployment and harmonization of risk assessment management. Moreover, the issue of access to classified information poses unique challenges to Europol's accountability as the principle of originator control, which governs access to classified information, creates an asymmetry between the European Parliament and national parliaments.

[4] The central piece of this legislation is the Regulation (EU) 2016/794 Europol Regulation (ER), which was amended on the 8th of June 2022 by Regulation (EU) 2022/991. It has particular focus on operational personal data, i.e. all personal data processed for the purpose of meeting the objectives of the Agency.

[5] Additionally, Europol applies Regulation (EU) 2018/1725to administrative personal data. Europol's data protection legal framework is based on the principles contained in Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as on the Council of Europe Committee of Ministers Recommendation No R (87) 15 regulating the use of personal data in the police sector

The paper employs a qualitative research methodology, utilizing a comprehensive review of legislative texts, policy documents, and relevant academic literature. Case studies of specific interactions between Europol and oversight bodies, such as the EDPS, provide practical insights into the application and effectiveness of the accountability framework. The analysis includes the legislative framework established by the Europol Regulation and the role of oversight bodies like the Joint Parliamentary Scrutiny Group (JPSG), as well as the analysis of the current accountability governance network established to oversee the activities of this enforcement organization. The author also recognize the paper limitations, including the rapidly evolving nature of EU legislation and policies, which may affect the relevance of some findings. Additionally, access to classified or sensitive information may constrain the depth of analysis in certain areas, yet, in a next step of this research, there is a plan to conduct in depth interviews and surveys to explore the accountability of EU security organizations including Europol. As conclusion, this study provides an examination of Europol's accountability mechanisms, assessing their effectiveness and identifying areas for improvement. By exploring the legislative framework, oversight practices, and specific governance challenges, the study aims to contribute to the ongoing discourse on enhancing accountability and transparency within this agency.

Part 1. Overview of Europol mandates

Regulation (EU) 2016/794 of the European Parliament and the Council, enacted on May 11, 2016, established the legal framework governing the European Union Agency for Law Enforcement Cooperation (Europol).[6] This regulation consolidated and updated the agency's mandate, replacing several previous Council Decisions. A critical aspect of the regulation is its emphasis on accountability, in the form of defining the main mandates and capabilities permeating its various provisions and operational guidelines.

The primary objective of Europol, as outlined in the regulation, is to support and strengthen the actions of member states' competent authorities in preventing and combating serious crime that affects two or more member states, as well as terrorism and other forms of crime that threaten a common interest covered by Union policy. This goal demands a high level of accountability from Europol, ensuring that its efforts are effective and coordinated with national authorities. The regulation extends Europol's objectives to include related criminal offences, such as those committed to procure means for acts within Europol's competence, facilitate or perpetrate such acts, or ensure impunity for those committing such acts. This extension requires Europol to maintain stringent oversight and justification for its involvement in these related offences, ensuring that its actions remain aligned with its primary objectives.

Europol's tasks, detailed in Article 4, are designed to achieve these objectives. Europol is tasked with collecting, storing, processing, analyzing, and exchanging information, including criminal intelligence. This extensive handling of information necessitates rigorous accountability measures to ensure data accuracy, protection, and proper use. Europol must notify member states promptly of any pertinent information and connections between criminal offences. This requirement underscores the need for transparency and reliability in Europol's operations, as timely and accurate information exchange is crucial for effective law enforcement cooperation (Busuioc & Groenleer, 2016).

[6] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on 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, available at https://eur-lex.europa.eu/eli/reg/2016/794/oj

Furthermore, Europol coordinates, organizes, and implements investigative and operational actions to support and strengthen the efforts of member states' authorities. These actions can be carried out jointly with national authorities or within the context of joint investigation teams. Accountability in these tasks involves clear communication, proper resource allocation, and adherence to legal standards. Europol's role in preparing threat assessments, strategic and operational analyses, and general situation reports also demands a high level of accountability, ensuring that the information provided is accurate, relevant, and useful for member states' law enforcement activities.

The regulation also empowers Europol to request the initiation of criminal investigations. In specific cases, where Europol believes a criminal investigation should be initiated, it can request the competent authorities of the concerned member states to initiate, conduct, or coordinate such an investigation. This provision requires Europol to have valid and well-substantiated reasons for its requests, respecting the decisions made by national authorities. National units are obliged to inform Europol of their decisions regarding these requests, fostering a transparent and cooperative relationship. If a member state decides not to accede to Europol's request, it must inform Europol of the reasons for its decision without undue delay, preferably within one month (Jansson, 2018). This process ensures mutual accountability between Europol and the member states, as Europol's requests must be justified, and member states' responses must be transparent and prompt.

Governance and oversight of Europol are structured to ensure accountability at the highest levels. The Management Board, as outlined in Article 10, comprises one representative from each member state and one representative from the European Commission, each with a voting right. Members of the Management Board are appointed based on their knowledge of law enforcement cooperation, ensuring that those governing Europol are well-informed and competent. The regulation also promotes gender balance on the Management Board, enhancing diversity and accountability in governance.

The functions of the Management Board, detailed in Article 11, include adopting Europol's multiannual programming and annual work program, adopting the annual budget, and exercising other budgetary functions. The Management Board also adopts a consolidated annual activity report on Europol's activities, which is sent to the European Parliament, the Council, the Commission, the Court of Auditors, and national parliaments, and is made public. These functions ensure that Europol operates transparently and is held accountable for its actions and expenditures (Deflem, 2006; De Moor & Vermeulen, 2010). The Management Board also adopts financial rules applicable to Europol and an internal anti-fraud strategy, ensuring fiscal responsibility and integrity. Additionally, the Board sets performance indicators and oversees the performance of the Executive Director, including the implementation of Management Board decisions.

At the same time, data protection is a critical aspect of Europol's operations, as the agency processes a significant amount of information, including personal data. Article 18 stipulates that Europol may process information, including personal data, only insofar as necessary to achieve its objectives. Personal data processing is restricted to specific purposes, such as cross-checking to identify connections between information, strategic or thematic analyses, operational analyses, and facilitating information exchange between member states, other Union bodies, third countries, and international organizations (Orlandi, 2021).

For operational analyses, specific safeguards are established. The Executive Director must define the specific purpose, categories of personal data, categories of data subjects, participants, duration of storage, and conditions for access, transfer, and use of the data for each operational analysis project. These details must be communicated to the Management Board and the European Data Protection Supervisor (EDPS), ensuring oversight and accountability. Personal data may only be collected and processed for the defined purposes of each operational analysis project. If personal data becomes relevant for another project, further processing is permitted only if it is necessary, proportionate, and compatible with the specified provisions. Only authorized staff may access and process data for these projects, maintaining strict control and accountability over sensitive information (Kaunert, 2010).

Article 19 further elaborates on the determination of the purpose and restrictions on the processing of information by Europol. When providing information to Europol, member states, Union bodies, third countries, or international organizations must specify the purposes for which the data will be processed. If the provider has not determined the purpose, Europol, in agreement with the provider, must determine the relevance and purposes of the information. Europol may only process information for a purpose different from that for which it was provided if authorized by the provider. Yet, providers of information can also impose restrictions on access or use, including transfer, erasure, or destruction of the data. Europol is required to comply with these restrictions, ensuring that the use of the information respects the conditions set by the providers (Fägersten, 2010). In cases where the need for such restrictions becomes apparent after the information has been provided, the providers must inform Europol accordingly, and Europol must adhere to these new restrictions.

In general, Regulation (EU) 2016/794 establishes a comprehensive framework for Europol's operations, emphasizing accountability through detailed objectives, clear tasks, structured governance, and data protection measures. Europol's mandate to support and strengthen law enforcement cooperation among EU member states is underscored by the attempt to promote transparency, data protection, and mutual accountability with national authorities and other stakeholders. Yet, it is necessary to deep into data protection aspects of this regulation, as this front has become one of the main regulatory aspects to turn Europol more accountable, especially in the face of big data and automated data processing.

Part 2. Data protection regulation

In terms of data protection, the Directive (EU) 2016/680, adopted by the European Parliament and the Council on April 27, 2016, established a comprehensive framework for the protection of natural persons concerning the processing of personal data by competent authorities for criminal law enforcement purposes. This directive aims to balance the necessity of data processing in law enforcement with the fundamental rights and freedoms of individuals, ensuring accountability at every stage. There is no aim in analyzing the whole text and implications of the Directive. Yet, some of the main important articles are covered as follows.

Article 7 of the Directive aim to provide a clear definition of ‘competent authorities’. These include any public authority responsible for preventing, investigating, detecting, or prosecuting criminal offences, executing criminal penalties, and safeguarding against public security threats. It also encompasses any other body or entity entrusted by Member State law to exercise such functions. By delineating the scope of competent authorities, the Directive ensures that only those entities with a legitimate mandate can process personal data for law enforcement purposes, promoting accountability and preventing misuse.

The roles of ‘controller’ and ‘processor’ in the regulation are also crucial to the Directive's framework. A controller is supposed to be a competent authority that determines the purposes and means of data processing, whether alone or jointly with others. This determination can also be specified by Union or Member State law. The processor, on the other hand, processes personal data on behalf of the controller. The definitions aims to establish clear lines of responsibility and accountability, ensuring that data processing activities are conducted under strict oversight and control. Yet, as discussed in the next sections, the controller’s primary role is critical because it holds ultimate responsibility for ensuring compliance with data protection principles and obligations.

To uphold the quality and integrity of personal data, Article also 7 requires competent authorities to verify the accuracy, completeness, and reliability of data before transmission or making it available. This includes adding necessary information to enable the receiving authority to assess the data's quality. This provision highlights the importance of data accuracy in law enforcement, ensuring that decisions are based on reliable information and protecting individuals from the adverse effects of incorrect data (Busuioc & Groenleer, 2016).

Article 10 is very important as it addresses the processing of special categories of personal data, such as those revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and data concerning a person's sex life or sexual orientation. Such processing is allowed only when strictly necessary, subject to appropriate safeguards, and authorized by Union or Member State law. The inclusion of strict necessity and appropriate safeguards underscores the Directive's commitment to protecting sensitive data and the rights of data subjects, aiming that such data is processed with the highest level of justification.

In the other hand, Automated Decision Making (ADM), including profiling, which significantly affects individuals, is restricted under Article 11. Such decisions are prohibited unless authorized by Union or Member State law and accompanied by appropriate safeguards, including the right to human intervention. This article ensures that individuals are not subjected to adverse decisions solely based on automated processing without adequate oversight and safeguards (Horii, 2018). It addresses the growing concern about the impact of automated decision-making on individual rights and emphasizes the need for human oversight in law enforcement decisions.

In that regard, article 20 introduces the principles of data protection by design and by default. Controllers are required to implement appropriate technical and organizational measures to integrate data protection principles effectively and safeguard data subject rights. This includes ensuring that only necessary personal data is processed by default. These measures must take into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing, as well as the risks posed to individuals. Yet, data protection by design and by default alone does not guarantee embedding data protection into the design and processing of ADM systems and practices (Birzu, 2019).

For example, the requirement for data protection impact assessments (DPIAs) in Article 27 further enhances accountability; as controllers must carry out DPIAs when processing is likely to result in high risks to individuals' rights and freedoms, particularly when using new technologies, even that there is no clear mention to big data or ADM. These assessments must include a general description of the processing operations, an evaluation of the risks, and the measures envisaged to address those risks. DPIAs serve as a tool for identifying and mitigating potential privacy risks before they materialize, ensuring that controllers take a proactive approach to protecting personal data. For this reason, article 28 stipulates that controllers or processors must consult the supervisory authority prior to processing that poses high risks, as identified by a DPIA. This prior consultation is necessary when the processing involves a new filing system or uses new technologies that could impact data subjects' rights and freedoms, such as DMA. This consultation mechanism try to ensure that high-risk processing activities receive additional scrutiny and oversight, promoting some degree of transparency and accountability.

In overall, Directive (EU) 2016/680 established a more robust framework for the protection of personal data processed by competent authorities for law enforcement purposes, likewise the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR). The Directive emphasizes a basic ground for accountability through the definitions of roles and responsibilities, rigorous data quality and accuracy requirements, strict controls on sensitive data processing, restrictions on automated decision-making, and the integration of data protection principles by design and by default. Additionally, the requirement for data protection impact assessments and prior consultation with supervisory authorities aim to ensure that potential risks are identified and mitigated proactively. In that sense, the Directive aims to balance the needs of law enforcement with the fundamental rights and freedoms of individuals, promoting at least a legal base to for responsibility and responsiveness in data processing activities.

Spotlighting critical points in Data Protection regulation

As mentioned, Directive (EU) 2016/680, aimed at regulating the processing of personal data by competent authorities for law enforcement purposes, is a significant step toward balancing security needs with individual privacy and individual rights. However, despite its comprehensive framework, several blind spots, pitfalls, and potential loopholes could undermine its effectiveness. A critical analysis of the Directive reveals these areas of concern. One of the primary blind spots in the Directive is its reliance on the definition of ‘competent authorities’. While it includes public authorities and other entities entrusted by Member State law, the broad nature of this definition could lead to inconsistent application across Member States.

This inconsistency may result in some entities being classified as competent authorities in one Member State but not in another, creating potential gaps in the protection offered by the Directive. This variability could be exploited, especially in cross-border cases, leading to uneven levels of data protection. In Germany, the Federal Police and Customs authorities are clear examples of competent authorities. However, smaller bodies like municipal law enforcement agencies might be considered competent authorities in one region but not in another. This inconsistency could lead to gaps in data protection, especially in cases involving cross-border data sharing. For instance, during the 2015 European migrant crisis, various local authorities collected and shared data with differing levels of oversight and protection, leading to potential privacy breaches (Horii, 2018).

Moreover, the distinction between the roles of ‘controller’ and ‘processor’ is another area of potential confusion. The Directive places significant responsibility on controllers to ensure compliance with data protection principles. However, in practice, the distinction between controllers and processors can be blurred, particularly in complex data-sharing arrangements such as ADM. This ambiguity could lead to situations where it is unclear which entity is responsible for safeguarding personal data, potentially resulting in accountability issues. Moreover, processors, despite their critical role, may not be held to the same rigorous standards, potentially creating vulnerabilities in data protection. In a multinational operation like Operation Sophia, aimed at curbing human smuggling in the Mediterranean, multiple agencies across different EU countries and international organizations work together. Determining which agency is the controller and which are processors can be challenging, leading to potential accountability issues. For instance, if an Italian naval unit shares data with Europol, but there is a breach, the responsibility might be unclear, confusing accountability and redress for affected individuals (Riekmann, 2016).

Furthermore, article 6 requires Member States to distinguish between different categories of data subjects, such as suspects, convicts, and victims. While this is intended to ensure appropriate handling of personal data, the practical implementation of these distinctions can be challenging. The nature of criminal investigations often involves fluid and evolving circumstances, making it difficult to categorize individuals accurately. Misclassification could lead to inappropriate data processing, with significant consequences for individuals wrongly identified as suspects or convicts. This challenge is compounded by the Directive's reliance on Member States to develop mechanisms for these distinctions, which may lead to inconsistent application and protection levels across units in different Member States. For instance, in the aftermath of the 2015 Paris attacks, French authorities collected data from thousands of individuals. Distinguishing between suspects, witnesses, and victims was difficult in the chaotic investigation phase. Misclassifications led to innocent individuals being treated as suspects, resulting in undue surveillance (Busuioc & Groenleer, 2016).

The Directive also mandates that personal data must be accurate, complete, and up-to-date (Article 7). Nevertheless, ensuring data quality, especially in dynamic and complex criminal investigations, is a significant challenge. The directive's requirement that competent authorities verify data quality before transmission is practical, but the fast-paced nature of criminal investigations may make this difficult. Delays in data verification can impede law enforcement operations, while insufficient verification can lead to the processing of inaccurate data, potentially harming individuals' rights and undermining the integrity of law enforcement activities. In the 2011 Norway attacks, the speed of data collection and dissemination led to inaccuracies. Some individuals wrongly identified as associates of the perpetrator were subject to unnecessary scrutiny. The rapid data sharing between Norwegian authorities and Europol without thorough verification exacerbated these issues, highlighting the difficulty in balancing timely law enforcement action with data accuracy (Busuioc & Groenleer, 2016).

On the other hand, article 10 is supposed to address the processing of special categories of personal data, such as racial or ethnic origin, political opinions, and health data. While the Directive requires that such processing is strictly necessary and subject to appropriate safeguards, these terms are open to interpretation. What constitutes 'strictly necessary' can vary, leading to potential overreach by competent authorities (Birzu, 2019). Additionally, the requirement for 'appropriate safeguards' is somewhat vague, leaving room for varied implementations that may not always provide adequate protection. This lack of specificity could be exploited, resulting in the processing of sensitive data without sufficient justification or protection.

Moreover, important to mention that the restrictions on Automated Decision Making (ADM) (Article 11) are a significant safeguard against potential abuses. However, the exceptions allowed, where such decisions are authorized by law, create a potential loophole. The Directive does not provide clear criteria for what constitutes appropriate safeguards in these cases, which could lead to varying interpretations and implementations across Member States. Furthermore, the increasing use of artificial intelligence and machine learning in law enforcement poses additional challenges. These technologies can introduce biases and errors, and the Directive may not fully address the complexities and risks associated with their use in automated decision-making processes. In the United Kingdom, the Metropolitan Police's use of facial recognition technology for public surveillance has raised many concerns (Riekmann, 2016). The system flagged individuals based on algorithmic assessments, some of which were erroneous, leading to wrongful detentions. Although the UK has left the EU, similar technologies are used across Europe (Ilbiz et al., 2017). The Directive's exceptions could allow such practices, provided they are authorized by national law, potentially undermining safeguards against erroneous or biased automated decisions (Carrapiço & Trauner, 2016).

In regard to ADM, data protection by design and by default (Article 20) is a forward-looking principle that aims to integrate data protection into the development of processing systems. However, its implementation can be challenging, particularly for smaller or resource-constrained authorities. The requirement to consider the state of the art and the cost of implementation can lead to varying levels of compliance, with some authorities potentially unable to meet the high standards envisaged by the Directive. This could result in a patchwork of protections, with some individuals benefiting from robust safeguards while others do not.

The requirement for data protection impact assessments (DPIAs) (Article 27) could be another critical safeguard. In theory, the effectiveness of DPIAs depends on the thoroughness of the assessments and the willingness of authorities to act on the findings. In practice, DPIAs can become a box-ticking exercise, conducted perfunctorily without genuinely addressing the risks identified. Moreover, there is no clear enforcement mechanism within the Directive to ensure that the recommendations from DPIAs are implemented, potentially rendering this safeguard ineffective. One recent case, yet outside the Europol scope, was the deployment of body-worn cameras by police forces in the Netherlands required DPIAs. Initial assessments highlighted significant privacy risks, particularly concerning the recording of minors and sensitive locations. However, due to operational pressures, some recommendations were not fully implemented, leading to instances where sensitive data were inadvertently captured and mishandled as in the case of migration controls and refugees asylum seekers procedures (Horii, 2018; Lazcoz & De Hert, 2023).

In terms of risk assessment, prior consultation with supervisory authorities (Article 28) is intended to provide an additional layer of oversight for high-risk processing activities. However, the Directive does not specify the criteria for what constitutes a high-risk activity in sufficient detail, leaving this determination to the discretion of the controllers. Again, this discretion can lead to inconsistent application and potential underreporting of high-risk activities. Furthermore, the capacity and resources of supervisory authorities to effectively oversee these consultations can vary significantly, potentially limiting their ability to provide meaningful oversight. When the Belgian police proposed integrating a new AI-driven crime prediction tool in a program called 'i-Police', they consulted the national data protection authority. Nonetheless, the assessment of high risk was subjective, and the authority's limited resources meant the consultation was not as thorough as needed. Consequently, the tool was implemented with insufficient safeguards, leading to potential profiling and discrimination issues.[7]

As seen above, Directive (EU) 2016/680 establishes a robust framework for protecting personal data within law enforcement activities. Yet, the broad and variable definitions, challenges in data subject categorization, ensuring data quality, vague requirements for sensitive data processing and automated decisions, practical difficulties in implementing data protection by design, DPIAs, and supervisory consultations pose significant challenges. Real examples were cited to illustrate these issues, emphasizing the need for ongoing vigilance, clear guidance, and consistent application to ensure the Directive effectively protects individuals' privacy rights while enabling efficient law enforcement. Addressing these blind spots, pitfalls, and potential loopholes is crucial for maintaining the Directive's integrity and effectiveness in the evolving landscape of data protection and law enforcement. Yet, more challenges arise when enforcement operations entail further data exchange that are conducted outside Data Protection scope.

Data Exchange outside Data Protection scope

Within the intricate legal framework governing Europol's operations, the provision outlined above stands as a pivotal base, dictating the parameters within which data exchanges occur between the competent authorities of Member States and private entities. This provision, while seemingly straightforward, encompasses a multitude of complexities and implications that warrant a stable judicial base for Europol activities. However, it is necessary to focus into the nuances of Article 6c, as this short article could unravel new details surrounding data protection, privacy rights, and

[7] Sopra Sterla was a contractor chosen by Belgian Integrated Police to drive its digital transformation through the i-Police program. Yet, a report found that the predictive tool does not contribute to security, rather, it brings uncertainty (every judge will handle it differently), and also brings inefficiency in the process to control and assess AI made evidence. See report "AI and Administration of Justice: Belgian Report for the 3th Section of IAPL" in https://penal.org/sites/default/files/files/A-09-23.pdf

accountability within the operational landscape of Europol. As mentioned in the Regulation (EU) 2016/794 Europol Regulation (ER), Article 6c:

> c. Europol's infrastructure may be used for exchanges between the competent authorities of the Member States and private parties in accordance with the respective national law. Those exchanges may also cover crimes that do not fall within Europol's objectives.
>
> Where Member States use Europol's infrastructure for the exchange of personal data on crimes that fall within Europol's objectives, they may grant Europol access to such data.
>
> Where Member States use Europol's infrastructure for the exchange of personal data on crimes that do not fall within Europol's objectives, Europol shall not have access to those data and shall be considered to be a processor in accordance with Article 87 of Regulation (EU) 2018/1725.[8]

As seen, at the heart of the matter lies Article 6c, a regulatory clause delineating the permissible scope of Europol's infrastructure utilization for data exchanges, including those extending beyond its primary mandates. This provision, though seemingly broad, carries profound implications, particularly concerning data protection, privacy rights, and the all-encompassing veil of accountability confusing Europol's operational modus operandi. In that sense, there is a clear stipulation that Europol's infrastructure may serve as a conduit for data exchanges between Member States' competent authorities and private entities, all under the purview of respective national legal frameworks. This broad mandate presents a spectrum of possibilities, ranging from seamless cooperation to potential disparities in data protection practices across Member States, underscoring the need for harmonization and cohesive interpretation.

Of particular concern is the provision which permits Europol's infrastructure to facilitate data exchanges involving offenses falling beyond the purview of its direct objectives. This potential expansion could saturate Europol with a broader mandate, extending its specialized focus beyond transnational crime and terrorism, potentially blurring the lines between legitimate law enforcement activities and unwarranted surveillance practices. Yet, in practical terms is difficult to foresee this scenario, as enforcement effort is conducted by the collaboration of Member States, rather by an obligation to centralize all the activities of a European police in this agency.

Yet, in those shared tasks, adding complexity to the equation is the threat of third-party exploitation, wherein external countries may seek to leverage Europol's infrastructure to share intelligence without adhering to the rigorous data protection standards mandated by EU legislation. Should Europol transition into a blind data processor, the risks of inadvertently facilitating the transfer of personal data without requisite safeguards loom large, thereby imperiling the fundamental rights of individuals enshrined within EU law (Brière, 2019; Cooper, 2018).

Illustrative of these risks is the hypothetical scenario wherein agreements akin to the EU-U.S. Privacy Shield facilitate bulk data sharing between the United States and Europol. Such agreements, stalled in legal ambiguities, could pave the way for the transmission of data concerning EU citizens, harvested under less stringent U.S. privacy laws, circumventing the robust protections mandated by EU legislation and potentially precipitating egregious breaches of privacy. Moreover, the nuanced role that Europol assumes as a data processor underscores the

[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, available in https://fusionforenergy.europa.eu/downloads/terms/Regulation_EC_2018_1725.pdf

inherent complexities in overseeing exchanged data, particularly when operating at a distance from the actual processing activities. This disconnect fosters an accountability vacuum, wherein neither Europol nor the Member States bear full responsibility for monitoring or rectifying instances of data misuse, perpetuating a state of regulatory ambiguity and uncertainty (Docksey & Propp, 2023).

Finally, by permitting data exchanges encompassing offenses diverging from its core objectives, Europol risks diluting its specialized focus on combating serious transnational crime and terrorism, potentially morphing into a generalized data exchange platform devoid of the initial purpose that reinforces its existence. Furthermore, the regulatory framework articulated within Article 6c, permitting data exchanges devoid of direct Europol access or involvement, creates a note of apprehension regarding data protection standards. Member States, vested with interpretive prerogatives, may lean towards prioritizing national security imperatives at the expense of law enforcement and privacy rights, potentially fostering a lax enforcement regime and challenging the robust safeguards mandated by EU legislation (Mitsilegas et al., 2023).

EDPS Decision on the own initiative inquiry on Europol's big data challenge

Within the realm of contemporary law enforcement, the advent of big data and Automated Decision-Making (ADM) has ushered in a new era of challenges and opportunities. At the forefront of this paradigm shift stands Europol, tasked with steering the complex interplay between technological advancements, data protection imperatives, and the exigencies of modern policing. Against this backdrop, a letter dated 17 November 2020, exchanged between Europol and the European Data Protection Supervisor (EDPS), serves as a focal point for examining the agency's accountability mechanisms in the realm of big data governance and ADM.

In a letter dated 17 November 2020,[9] Europol shared with the European Data Protection Supervisor (EDPS) the Action Plan requested under point 5.8 of the EDPS Decision from 17 September 2020, which relates to the EDPS's own inquiry into Europol's big data challenge. In this text, Europol informed the EDPS that the Action Plan would be discussed with the Europol Management Board (EMB) during their next meeting in December 2020 and requested feedback regarding its implementation. The EDPS expressed appreciation for Europol's efforts in developing the Action Plan within the two-month deadline set by the EDPS Decision of 17 September 2020. After a detailed analysis, the EDPS acknowledged that the Action Plan includes strong elements to address the risks associated with processing large datasets at Europol.

However, the EDPS noted that some elements require further clarification or specification and indicated a willingness to provide additional comments to help improve these areas. The EDPS also expressed regret that Europol had not shared the accompanying data protection risk assessment, which hampers the EDPS's ability to fully evaluate whether the existing controls sufficiently address all data protection risks involved. The European Data Protection Supervisor (EDPS) raised significant concerns about Europol's handling of large datasets, particularly in terms of data protection and compliance with existing regulations.

The following paragraphs critically examines the EDPS's letter addressing Europol's Action Plan, which was crafted in response to an inquiry into Europol's big data practices. The assessment focuses on four main controls identified by the EDPS: flagging datasets in SIENA, labelling of big data files, restricting access rights to raw data, and increasing the frequency of data reviews.

[9] Cases 2019-0370 & 2021-0699, EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorization, available in https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf

Firstly, the flagging of large datasets in SIENA was identified as a foundational control for all subsequent measures. SIENA stands for "Secure Information Exchange Network Application." It's a platform used by Europol for secure communication and information sharing among law enforcement agencies across the European Union. The EDPS underscored the crucial role of data providers in identifying datasets that cannot undergo the regular data classification process. The ambiguity in Europol's commitment to implementing the necessary technical changes in SIENA was found problematic. On it, the Action Plan indicates that Europol is only exploring the possibility of these updates, rather than committing to them. This lack of commitment raised concerns about the plan's effectiveness, as the success of subsequent controls hinges on the proper implementation of this first step. The EDPS urges Europol to either clearly commit to the SIENA update or outline alternative measures. Furthermore, there is a need for detailed measures to ensure that the flagging process is conducted and monitored correctly. The EDPS also requested access to the ICT work planning for the next years to assess the timeline and content of the SIENA update, emphasizing the importance of transparency and accountability in the implementation process.

The second control, the labelling of big data files in Europol’s data environment, is considered even more critical, as it dictates the applicability of all other measures. The EDPS notes that the Action Plan lacks clarity on whether Europol will establish a maximum retention period for datasets awaiting flagging. This omission is significant because indefinite retention of data can lead to unnecessary risks and potential breaches of data protection regulations. Additionally, the plan focuses on the process preceding the analysis work, with only a dedicated number of analysts accessing raw data for classification purposes. The EDPS was concerned about the potential risks of processing data without a clear data subject classification (DSC) and the likelihood of such risks occurring. The labelling process should address these risks by preventing unclassified data from being further processed or integrated into analysis work. However, the Action Plan lacks specifics on the measures to enhance the confidentiality of raw data, such as encryption, and the monitoring mechanisms to ensure that labelling is performed correctly.

Regarding the restriction of access rights to raw data, the EDPS views this control as a strong safeguard against the further processing of unclassified data. Limiting access to a select group of analysts is intended to minimize risks and ensure compliance with data protection regulations. However, the EDPS seeks further information on several points. It questioned the criteria used to define who will have access to the data and the "need-to-know" basis for this access. This information is crucial for understanding how Europol ensures that only authorized personnel handle sensitive data (Drewer & Miladinova, 2017; Jannson, 2018). The EDPS also inquired, in the same document, about the time limits imposed on the extraction task and the specific activities involved in the review performed by the analysts. Another concern was the policy regarding the deletion of raw data after the relevant information has been extracted. If the data is stored to preserve the chain of evidence, it is important to know whether Europol plans to store this data in a separate functional environment to ensure it is adequately protected.

The fourth control involved increasing the frequency of data reviews at the level of Analysis Projects (APs). The EDPS agreed that regular reviews are necessary to assess the necessity and proportionality of storing unclassified data. However, it expresses strong reservations about the efficiency of this control as described in the Action Plan. The criteria for assessing the relevance of datasets are the same as those for extracted data, which have already undergone an initial assessment of necessity and proportionality. This approach may not be feasible in practice, as assessing the necessity and proportionality of unclassified data without knowing its content is challenging (Drewer & Miladinova, 2017). The EDPS suggests that the review process should be stricter and include clear criteria, such as imposing a maximum time limit for storage. The EDPS's concerns are compounded by past experiences, noting that previous recommendations regarding data deletion have not been fully implemented. This claim raises doubts about Europol's ability to effectively delete datasets that fail the review test. The Action Plan also lacks specifics on the frequency of reviews and how datasets deemed unnecessary or disproportionate should be managed to preserve the chain of evidence.

Finally, the appointment of a Data Quality Control Coordinator is welcomed by the EDPS as a positive step toward ensuring efficient data review mechanisms. This role is crucial for monitoring the implementation of the data review process and acting in close collaboration with the Data Protection Function. The EDPS highlights the need for sufficient resources to be allocated to the data review process, given the volume of personal data processed at Europol and the significant workload involved (Voss, 2021). While the appointment of a coordinator is a positive development, it is not sufficient on its own to ensure an effective review process. The Data Quality Control Coordinator should have a strong action plan in place to ensure comprehensive and efficient review mechanisms (McDaniel & Lavorgna, 2019). Hence, the EDPS requested a full description of the coordinator's tasks and a copy of the action plan to assess the robustness of these mechanisms.

In short, while the Europol Action Plan addresses several key areas of concern, there are significant gaps and ambiguities that need to be addressed to ensure robust data protection practices. The lack of a firm commitment to implementing necessary technical changes, unclear retention periods for unclassified data, insufficient details on risk assessment and mitigation measures, and concerns about the effectiveness of review processes all highlight areas for improvement. Europol, according to the EDPS, must provide clearer commitments, detailed implementation plans, and robust oversight mechanisms to meet the data protection standards expected by the EDPS.

And this front is of especial concern, especially if we consider that not only coordination dilemmas between Europol and the EDPS can undermine accountability. That is, there is also the risk of technical mandates being undermining the real accountability from this organization. For example, one of the main aspects in this regard come from Automated Decision Making (ADM). In this regard, there is a potential of creating legal mask to just produce informs of risk assessment and data protection, whereas real assessment of the data quality, data breaches, the proportionality of the operations, and the privacy but also individual safeguards against algorithmic discrimination still can be covered for the sake of risk mitigation (Brière, 2019). That is, it is crucial that Automated Decision Making (ADM) will not become an ongoing checklist to accomplish data protection rules; rather, it is supported that ADM should be addressed as a contextual practice (not only as a technical mechanism) in the whole accountability chain and governance network in which Europol and other security organizations are merged (Jannson, 2018).

In the light of that, what is perhaps being observed through the letter is not the delegation of critical (high-risk) decisions to machines without any human involvement. Instead, individuals making pressured decisions could be presented with empirical risk rankings, the reasoning behind which they cannot question. This issue is pervasive across most Decision-Making (DM) systems, regardless of whether they are fully automated or involve human intervention. Automation bias significantly constrains the effectiveness of human intervention, limiting its capacity to meaningfully address concerns associated with Automated Decision-Making (ADM) systems. Yet, some scholars like Quintel (2020) and Coman-Kund (2021) argue that relying solely on human agents to address or mitigate these concerns is not feasible. In their examination of this regulatory landscape, they aim to confront its shortcomings contending that human intervention alone is important but insufficient for achieving adequate human oversight of these systems. In other words, human intervention is ineffective if is not complemented by accountability governance in other phases of the organization management and operations. In that sense, current risk assessment and data protection rules encompass accountability as a technical means for data processing and sharing, whereas accountability should be also a meta-objective for information and governance practices.

Part 3. Accountability governance: beyond risk management

The effective governance of Europol, the European Union Agency for Law Enforcement Cooperation, hinges on specific mechanisms that aim to ensure accountability and compliance. Articles 41 to 51 of the Europol Regulation, for instance, delineate the roles and responsibilities of key actors involved in overseeing Europol's activities, ranging from the appointment and tenure of the Data Protection Officer (DPO) to parliamentary scrutiny of the agency's operations. This part provides an overview of the critical provisions outlined in these articles, underscoring their significance in promoting transparency, accountability, and democratic legitimacy within Europol's framework. Then we discuss critical blind spots on this governance, assessing the current governance schemes in the issue of risk management, as it has become the main policy under data protection rules and Europol activities to manage and share data.

Governance in the accountability of Europol

The main regulations to establish accountability governance of Europol are established in the Regulation (EU) 2016/794 explained in part 1. Yet, here we address articles 41 to 51 as these are focused on the external accountability of this enforcement agency. For example, article 41 of the Europol Regulation outlines the crucial role of the Data Protection Officer (DPO) in ensuring accountability and compliance with data protection regulations within the organization. By this, the Management Board is tasked with appointing a DPO who possesses the requisite personal and professional qualities, including expert knowledge of data protection. Importantly, the DPO is expected to act independently in the performance of their duties, free from conflicts of interest that may arise from other official responsibilities.

Furthermore, the appointment of the DPO is subject to specific tenure requirements, with a term of four years and eligibility for reappointment for up to eight years in total. Dismissal of the DPO from their function can only occur with the consent of the European Data Protection Supervisor (EDPS), emphasizing the need for robust accountability mechanisms in overseeing the DPO's role. The responsibilities of the DPO, as delineated in Article 41(6), are instrumental in ensuring effective data protection practices within Europol. These include overseeing the internal application of data protection regulations, maintaining records of data transfers, informing data subjects of their rights, collaborating with Europol staff and the EDPS, preparing annual reports, and managing a register of personal data breaches. These tasks underscore the DPO's pivotal role in upholding data protection standards and promoting accountability within Europol.

At the same time, Article 42 establishes the role of national supervisory authorities in independently monitoring the permissibility of data transfers to Europol by Member States. These authorities are granted access to relevant data and documentation to facilitate their supervisory functions, ensuring compliance with national laws and protection of data subjects' rights. Additionally, national supervisory authorities are required to inform the EDPS of any actions taken with respect to Europol, facilitating coordination and cooperation between national and European oversight bodies (Rosano, 2016).

Supervision by the EDPS, as outlined in Article 43, further reinforces accountability measures within Europol. The EDPS is responsible for monitoring and ensuring compliance with data protection provisions, investigating complaints, conducting inquiries, advising Europol and data subjects, and maintaining a register of processing operations. The EDPS's authority to access personal data and premises at Europol, as well as their obligation to produce annual reports, enhances transparency and accountability in data processing activities. Cooperation between the EDPS and national supervisory authorities, as mandated by Article 44, is essential for addressing discrepancies and ensuring consistent application of data protection standards across Member States, one example of this is the mentioned EDPS decision inquiring Europol in the face of big data challenges and risk assessment actions in 2022. The establishment of the Cooperation Board, composed of representatives from national supervisory authorities and the EDPS, further facilitates dialogue and collaboration on data protection policies and strategies. Whereas Article 51 of the Europol Regulation introduces an essential component of accountability: parliamentary scrutiny. This mechanism ensures that Europol's activities are subject to oversight by both the European Parliament and national parliaments, reflecting the importance of democratic control in the organization's operations (Piquet, 2021).

To create a more consistent accountability governance and link with the representatives of the people, the Joint Parliamentary Scrutiny Group (JPSG) is established under Article 51(1), comprising representatives from the European Parliament and national parliaments. This group is tasked with politically monitoring Europol's activities, focusing on its mission and the impact of its actions on the fundamental rights and freedoms of individuals. Essentially, the JPSG has the authority to request appearances by key figures within Europol, such as the Chairperson of the Management Board or the Executive Director, to discuss various matters, including budgetary aspects and organizational structures. Additionally, the European Data Protection Supervisor (EDPS) is required to appear before the JPSG at least once a year to discuss matters related to data protection and privacy, highlighting the significance of these issues in parliamentary oversight (Piquet, 2021). This is explained because Europol, as an EU agency, is subject to the ordinary legislative procedure, wherein the European Parliament (EP) and the Council determine the structure, operation, field of action, and tasks of the agency, including arrangements for inter-parliamentary oversight. Additionally, Europol operates with an autonomous budget, primarily funded through contributions from the general budget of the Union, subject to the general EU budget procedure. The agency drafts its budget plans, which are then submitted to the European Parliament and the Council for approval of appropriations, as outlined in Article 58 of the Europol regulation (Schinina, 2020).

Moreover, Article 51(2) specifies that the JPSG needs to be consulted regarding the multiannual programming of Europol, ensuring parliamentary input into the strategic planning process of the organization. This provision enhances more transparency and accountability by allowing elected representatives to contribute to Europol's long-term objectives and priorities. In summary, the last two articles aim to establish a robust framework for parliamentary scrutiny of Europol's activities, encompassing both European and national levels of governance. By providing parliamentary representatives with the authority to monitor Europol's actions, participate in decision-making processes, and address fundamental rights concerns, this mechanism reinforces accountability and democratic legitimacy within the organization. At the time of this writing, some of the parliamentary oversight reports are published in the website of Europol, in which the query "parliament" retrieves 13 entrances with diverse information. For instance, Consolidated Annual activity Report (CAARs), Europol Budget information, Information concerning activities of senior staff members after leaving the service, and updates on current parliamentary regulations or policy reports, such as the European Union Situation and Trend Report (TESAT), alongside the Annual Transparency Reports released by the agency since 2017.

Potential governance pitfalls

There is no aim in assessing each of the reports and policy documents worked between Europol and the accountability holders. Yet, for the sake of this paper, it is important to address the main critical points and aspects that were constructed in the current legal governance of accountability from this agency. That is, the Europol Regulation, spanning Articles 41 to 66, presents a multifaceted framework aimed at governing data protection, supervisory oversight, and accountability within the organization. Article 41, as mentioned, mandates the appointment of a Data Protection Officer (DPO), tasked with acting independently and possessing expert knowledge in data protection. While this provision signifies a commitment to internal oversight, questions may arise regarding the extent of the DPO's independence, especially if their appointment process lacks robust safeguards against external influence or conflicts of interest (Carrapiço & Trauner, 2016).

Similarly, article 42 outlines the role of national supervisory authorities in monitoring the transfer, retrieval, and communication of personal data to Europol. While these authorities are intended to provide independent oversight, variations in national laws and enforcement capacities across Member States could affect the consistency and effectiveness of their supervisory functions. Harmonizing practices and resources among national supervisory authorities is then crucial to ensure uniformity in data protection standards.

On the other hand, article 43 entrusts the European Data Protection Supervisor (EDPS) with monitoring and enforcing data protection provisions within Europol. While the involvement of the EDPS could enhance accountability, coordination challenges between the EDPS and national supervisory authorities may arise as seen in Part 2 of this study. Clear mechanisms for cooperation and information-sharing are essential to address discrepancies and ensure a harmonized approach to data protection supervision. That is, challenges persist in ensuring uniform compliance across member states and preserving the independence of supervisory (Voss, 2021). In relation to article 45, which establishes a Cooperation Board comprising representatives from national supervisory authorities and the EDPS, National supervisory authorities are tasked with monitoring data transfers to Europol, while the EDPS oversees compliance with data protection regulations. Yet, while this initiative fosters dialogue and collaboration, the advisory nature of the Cooperation Board still needs to strive its influence on decision-making processes within Europol authorities and harmonize the monitoring of data transfers (Carrapiço & Trauner 2016).

It was also mentioned that Article 51 establishes a Joint Parliamentary Scrutiny Group (JPSG) composed of representatives from the European Parliament and national parliaments. While the JPSG aims to politically monitor Europol's activities, its effectiveness may be contingent upon the cooperation and engagement of relevant stakeholders. Balancing the need for discretion and confidentiality with the imperative of democratic oversight poses a significant challenge in this regard. Furthermore, if parliamentary scrutiny constitutes a fundamental pillar of democratic oversight over Europol's activities, the establishment of the Joint Parliamentary Scrutiny Group (JPSG) aims to provide political oversight, including budgetary matters and structural organization. Yet, the effectiveness of parliamentary scrutiny mechanisms hinges on the active engagement of national parliaments and the European Parliament. Strengthening the role of the JPSG and promoting transparency in Europol's operations are still critical to enhancing democratic accountability (Piquet, 2021). Also, it is important to tackle the accountability of key policy sectors that contribute to the work of the enforcement agency. Jannson (2018) supports that the EP has overlooked the oversight of partner systems, such as the European Union Agency for Criminal Justice Cooperation (Eurojust), and focused on supervising policing agencies such as Europol. In that sense, the accountability of Europol should serve to foster the oversight of the cooperation between judicial systems and avoid misuse of sources or potential corruption.

Another limitation may stem from the regulations governing access to classified information. The first challenge arises from the existing disparity between the European Parliament (EP) and national parliaments in accessing such information. A more general issue relates to the European Union's rules on classified information. Europol primarily relies on data provided by national authorities, over which Member States maintain full control, governed by the principle of ‘originator control' (Orlandi, 2021). This principle dictates that the EP may be denied access to classified information if the originating authority withholds consent for disclosure, even if the information is relevant to the agency or impacts fundamental rights. This principle, while essential for facilitating information exchange within the security and intelligence community, poses a barrier to parliamentary access to classified data (Schinina, 2020).

Additionally, transparency provisions outlined in Article 66, such as the application of Regulation (EC) No 1049/2001 to Europol documents, contribute to accountability by promoting openness and accessibility of information. Nevertheless, concerns may arise regarding the potential limitations on transparency, particularly in cases where disclosure could compromise operational integrity or confidentiality. Striking a balance between transparency and operational imperatives is essential to uphold accountability while safeguarding sensitive information, but the latter cannot hamper the work of oversight and access to information from accountability holders. In this regard, as part of its mandate, Europol collects and processes vast amounts of data, raising important considerations regarding accountability and data protection. In recent years, the European Data Protection Supervisor (EDPS) has exerted increasing pressure on Europol to ensure compliance with data protection regulations, leading to a significant impact on the organization's corporate risk profile (Orlandi, 2021). For example, during the mentioned report from 2022, Europol faced several instances where it received opinions and recommendations from the EDPS, highlighting data protection concerns and necessitating corrective actions. To this case, more instances emerged in the last years as proof of the complexities involved in balancing law enforcement objectives with access to information and the protection of individuals' privacy rights.

For instance, regarding Europol's participation in the European Police Records Information System (EPRIS) and the Automation of Data Exchange Processes (ADEP), discussions between Europol and project partners ensued to address data protection concerns raised by the EDPS and the European Data Protection Board (EDPB), emphasizing the importance of collaboration in ensuring compliance (Ilbiz et al., 2017). In another instance, the EDPS issued an opinion in 2022 on implementing searches with fingerprints in the Schengen Information System (SIS) (Ilbiz & Kaunert, 2022). Europol responded to the observations and re-submitted documentation for consultation, ultimately receiving a positive opinion from the EDPS. Europol committed to implementing recommendations to ensure compliance by the scheduled operational date of SIS II recast.

The EDPS also issued an opinion on the Police Exchange of Records and Criminal Information (PERCI) project, outlining additional requirements for Europol to meet before its implementation. Europol developed a technical solution to address EDPS requirements, emphasizing the need to mitigate the risk of third-party access to personal data. Europol engaged in discussions with the EDPS to obtain feedback on the proposed solution, highlighting its commitment to addressing data protection concerns (Ilbiz & Kaunert, 2022). Lastly, the EDPS issued an opinion on the Querying Europol Systems with Enhanced Techniques (QUEST+) project, prompting Europol to provide a more detailed description of processing operations and related data protection risks.

Overall, these recent cases above underscore the challenges faced by Europol in steering the intersection of law enforcement priorities, data protection requirements, and the governance of accountability. The governance pitfalls and corrective measures arise from coordination dilemmas, compliance with regulation, especially in the case of data protection, and the ongoing development of technologies that could affect enforcement activities. In that sense, Europol’s willingness to engage with the EDPS and address concerns could reflect a commitment to upholding individuals' privacy rights while fulfilling its mandate to combat crime effectively. Yet, continued collaboration and accountability between Europol and public authorities, especially in the realm of data processing and sharing, still relies on risk management and compliance.

Risk management governance and further challenges

In the last years, Europol took significant steps to strengthen its risk management practices by introducing a comprehensive risk management policy and revising its corporate risk management process. Within Europol, a risk is defined as an uncertain event or series of events that, if they were to occur, could impact the organization's ability to achieve its objectives outlined in its annual business planning, including the Programming Document, Work Programme, and the Europol Strategy 2020+. This newly established policy outlines universal principles for corporate risk management, aimed at fostering a continuous and systematic approach to identifying and managing risks across the organization. This framework provides practical guidance for assessing risks, defining roles and responsibilities, and establishing workflows for risk assessment, all of which are integrated into Europol's quarterly performance reporting cycle (Coman-Kund, 2021).

In addition to regular quarterly risk reporting, Europol's corporate risk management strategy also addresses risks with broad organizational implications that are identified on an ad hoc basis. However, despite these proactive measures, Europol's corporate risk profile in 2022 revealed some key challenges. One significant issue was the increasing mandate and tasks assigned to Europol, coupled with a demand that exceeded the organization's available staffing levels (Mitsilegas et al., 2023). This imbalance posed risks to Europol's ability to fulfill its obligations, such as implementing the amended Europol Regulation and EU Interoperability, while also meeting stakeholder expectations effectively. Furthermore, there was a rising demand for the successful delivery of key ICT infrastructure solutions necessary for processing operational personal data, including the Data Analysis Portal (DAP), facial recognition technology, machine learning tools, the mentioned PERCI, and the use of Cloud services (Ilbiz & Kaunert, 2022).

It is clear that the policy's establishment of universal principles for corporate risk management demonstrates Europol's commitment to ensuring consistency and standardization in its approach to risk across the organization. This systematic and continuous approach to risk management is essential for effectively anticipating and addressing potential threats to Europol's operations and objectives. The practical guidance provided by the corporate risk management process facilitates the assessment of risks and clarifies roles, responsibilities, and workflows for risk assessment throughout the organization. By integrating risk assessment into its quarterly performance reporting cycle, Europol aims to ensure that risk management remains an ongoing and integral aspect of its operational activities.

However, despite these positive aspects, Europol's corporate risk profile in 2022 revealed several key challenges that warrant critical assessment, as the organization faced increasing mandates and tasks in staffing levels, posing a risk to its ability to fulfill obligations and meet stakeholder expectations. This could represent an imbalance between demand and resources highlights potential vulnerabilities in Europol's capacity to effectively execute its responsibilities. Furthermore, the reliance on key ICT infrastructure solutions for processing operational personal data, such as the Data Analysis Portal (DAP) and facial recognition technology, exposes Europol to risks stemming from external dependencies and suppliers. The organization's inability to mitigate these dependencies could compromise the reliability and security of its data processing activities, thereby undermining its effectiveness in combating cross-border crime and terrorism.

Finally, as expressed above, the problem of processing large amounts of data based on Automated Decision Making still possess a considerable challenge. What is being observed since the GDPR and data protection rules for law enforcement purposes is not the delegation of critical (high-risk) decisions to machines without any human involvement. Instead, individuals making pressured decisions are presented with empirical risk rankings, the reasoning behind which they cannot question. This issue is more pervasive across most Decision-Making (DM) systems, regardless of whether they are fully automated or involve human intervention (Orlandi, 2021; Mitsilegas et al., 2023). Automation bias significantly constrains the effectiveness of human intervention, limiting its capacity to meaningfully address concerns, but this especially more concerning in the use of third tools for Automated Decision-Making (ADM) systems.

In practice, this requires that the risk assessment policy outlined goes beyond mere transparency or establishing a human connection in ADM for the sake of data protection (as in the form of control by data subjects themselves in the domain of data protection). That is, it's important to note that control, as defined in the GDPR (General Data Protection Regulation), doesn't mean individuals have absolute control over their personal data. Rather, it refers to their ability to participate in and influence the data processing activities. Governance mechanisms, such as those outlined in Article 22(3) of the GDPR, utilize transparency as a tool to empower data subjects, allowing them to exercise other rights recognized in the regulation and exert influence over decision-making processes. The essence of dignity lies in the act of exercising influence: while human intervention by the data controller is a prerequisite, it is the ability of the data subject to exert control that truly embodies dignity in this context.

And here relies part of the problem, as data subjects in ADM have their rights sorted and hampered by a double layered obstacle: the automatic processing of their data, and that security or serious crime constitute and exception to the exercise of this right. Thus, some scholars argue that relying solely on data protection and human agents to address ADM in order to address or mitigate these concerns is not feasible (Lazcoz & De Hert, 2023). In the examination of the mentioned regulations, they contend that human intervention alone is insufficient for achieving adequate human oversight of ADM systems. Instead of a data protection framework centered in risk assessment, the focus should rely on accountability in the whole data and governance process. That is, accountability should be moved not only in the interaction between humans and machine, but also in the interaction between data processors, data controllers, data subjects and oversight bodies. The basic difference is because risk is oriented on security and anticipating threats whereas accountability could encompass these dimensions but also promote more transparency, responsibility, contestability, and even empowerment. Human governance is essential for effective operation but insufficient as accountability still need to play a pivotal role in the whole landscape (Lazcoz & De Hert, 2023). For example, the current challenge of Europol would consists of harmonizing risk assessment internal operations and outline the external accountability of Automated Decision Making (ADM) used in law enforcement, showing to DPAs and other actors the accomplishment of risk management solutions at the core of data protection. Yet, risk management alone and human intervention of ADM are not sufficient to avoid misuse of information, potential violation of privacy and individual rights, or even to mitigate the unbalance of power between data subjects and data processors. Hence, accountability should be an input and encompass data protection, risk assessment, and automation, instead of being an output or a checklist to achieve these.

Conclusion

The accountability of Europol, the European Union Agency for Law Enforcement Cooperation, is a subject of major importance in ensuring the agency's operations are conducted transparently, lawfully, and with due regard for the rights of individuals. Established to facilitate cooperation among EU member states in combating serious international crime and terrorism, Europol's role requires a robust framework of oversight and accountability to maintain public trust and operational integrity. This paper assessed the legislative and governance structures that underpin Europol's accountability, scrutinizing the effectiveness and challenges of these mechanisms in the face of big data and Automated Decision Making (ADM).

The paper discussed the main regulation and the pitfalls in the oversight of the enforcement agency considering Europol mandates, Data Protection rules, and data exchanges outside data protection rules. Moreover, it was discussed the role of accountability governance with other actors, such as the Joint Parliamentary Scrutiny Group (JPSG), the Management Board, data protection authorities from state members, and the European Data Protection Supervisor (EDPS). The interaction between Europol and the EDPS is illustrative of this broader oversight ecosystem. In 2022, Europol faced significant pressure from the EDPS regarding several high-profile projects. The EDPS issued opinions raising concerns about data protection and requiring Europol to make adjustments to ensure compliance. These interactions underscore the dynamic nature of regulatory oversight and the ongoing need for Europol to adapt its practices in response to supervisory feedback. For instance, the EPRIS.ADEP pilot project, which allows Member States to conduct pseudonymized checks against each other's databases, required extensive discussions and adjustments to address the data protection concerns raised by the EDPS and the European Data Protection Board (EDPB).

Another critical aspect of Europol's accountability is its risk management policy. In 2022, Europol introduced a comprehensive risk management policy and revised its corporate risk management process description. This framework is integral to Europol's quarterly performance reporting cycle, ensuring that risks are regularly assessed. The implementation of the risk management policy revealed several key elements characterizing Europol's corporate risk profile. One significant risk is the increasing mandate and tasks directed at Europol, which are not sufficiently matched by the required staffing levels. This mismatch creates challenges in meeting Europol's obligations and stakeholder expectations, particularly concerning the implementation of the amended Europol Regulation and EU Interoperability. Additionally, there is a rising demand for the successful delivery of key ICT infrastructure solutions for processing operational personal data, such as the Data Analysis Portal (DAP), facial recognition, machine learning tools for operational analysis, and the use of cloud services. These demands are further complex by external dependencies beyond Europol's control, highlighting the complexity of managing such risks effectively.

Moreover, the governance of human intervention in automated decision-making (ADM) systems is another critical area of concern. While ADM systems can enhance efficiency and accuracy, they also pose significant challenges, particularly regarding accountability and oversight. The influence of automation bias on human agents and the limitations of human intervention highlight the need for robust governance mechanisms. Article 22(3) of the General Data Protection Regulation (GDPR) emphasizes the importance of human intervention governance, using transparency as a means to provide data subjects with the opportunity to exercise their rights and influence decision-making processes. However, this opportunity is limited by the risk assessment orientation of data controllers and a transparency oriented for data protection, instead of an accountability in which all the cycle of security and information is covered by a multi-level governance between stakeholders.

Finally, the issue of access to classified information poses another layer of complexity in the accountability framework. Europol relies heavily on information provided by national authorities, which is subject to the 'principle of originator control.' This principle means that the European Parliament (EP) cannot access classified information if the originator denies consent for disclosure, even if the information impacts fundamental rights. This situation creates an asymmetry between the EP and national parliaments in accessing classified information, posing challenges to effective parliamentary oversight.

In short, this study shown that Europol Regulation provides the legal basis for these mechanisms, while bodies such as the EDPS and the JPSG play crucial roles in oversight. Yet, the introduction of comprehensive risk management policies and the emphasis on human intervention governance oriented for data protection tasks could reflect Europol's challenges to addressing the complexities of modern law enforcement. This paper aimed to provide a detailed analysis of these accountability mechanisms, exploring their effectiveness and identifying areas for improvement in the context of Europol's evolving mandate and operational environment.

References

Birzu, B. (2019). Cooperation between member states and Europol. *Tribuna Juridică*, *9*(18), 33-43.

Brière, C. (2019). Cooperation of Europol and Eurojust with external partners in the fight against crime: a legal appraisal. In *The External Dimension of EU Agencies and Bodies* (pp. 59-77). Edward Elgar Publishing.

Bruggeman, W. (2002). Policing and accountability in a dynamic European context. *Policing & Society*, *12*(4), 259-273.

Busuioc, M., & Groenleer, M. (2016). Beyond design: The evolution of Europol and Eurojust. In *Justice and Home Affairs Agencies in the European Union* (pp. 13-32). Routledge.

Carrapiço, H., & Trauner, F. (2016). Europol and its influence on EU policy-making on organized crime: Analyzing governance dynamics and opportunities. In *Justice and Home Affairs Agencies in the European Union* (pp. 85-99). Routledge.

Coman-Kund, F. (2021). Holding Europol accountable: The promise and challenges of (hybrid) multilevel accountability. In *Technocracy and the Law* (pp. 285-314). Routledge.

Cooper, I. (2018). A new form of democratic oversight in the EU: The joint parliamentary scrutiny group for Europol. *Perspectives on Federalism*, *10*(3), 184-213.

Deflem, M. (2006). Europol and the policing of international terrorism: counter-terrorism in a global perspective. *Justice quarterly*, *23*(3), 336-359.

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4).

Docksey, C., & Propp, K. (2023). Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective. *Oslo Law Review*, (1), 1-34.

Drewer, D., & Miladinova, V. (2017). The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation. *Computer law & security review*, *33*(3), 298-308.

Fägersten, B. (2010). Bureaucratic resistance to international intelligence cooperation–the case of Europol. *Intelligence and National Security*, *25*(4), 500-520.

Horii, S. (2018). Accountability, dependency, and EU agencies: The hotspot approach in the refugee crisis. *Refugee Survey Quarterly*, *37*(2), 204-230.

Ilbiz, E., & Kaunert, C. (2022). Europol and cybercrime: Europol's sharing decryption platform. *Journal of Contemporary European Studies*, *30*(2), 270-283.

Ilbiz, E., Kaunert, C., & Anagnostakis, D. (2017). The counterterrorism agreements of Europol with third countries: Data protection and power asymmetry. *Terrorism and Political Violence*, *29*(6), 967-984.

Jansson, J. (2018). Building resilience, demolishing accountability? The role of Europol in counter-terrorism. *Policing and Society*, *28*(4), 432-447.

Kaunert, C. (2010). Europol and EU counterterrorism: International security actorness in the external dimension. *Studies in conflict & terrorism*, *33*(7), 652-671.

Lazcoz, G., & De Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities. *Computer Law & Security Review*, *50*, 105833.

McDaniel, J. L., & Lavorgna, A. (2019). Enhancing the accountability and transparency of transnational police cooperation within the European Union. In *The Development of Transnational Policing* (pp. 73-99). Routledge.

Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2023). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, *29*(1-2), 176-211.

Orlandi, E. (2021). Corporate Governance in EU Agencies: The Europol Case. *International Journal of Operations Management*, *1*(4), 33-44.

Piquet, A. (2021). Agencies' reputational game in an evolving environment: Europol and the European Parliament. *Politics and Governance*, *9*(3), 85-95.

Quintel, T. (2020). Interoperable data exchanges within different data protection regimes: the case of europol and the european border and coast guard agency. *European Public Law*, *26*(1).

Riekmann, S. P. (2016). Security, freedom and accountability: Europol and Frontex. In *Security versus Justice?* (pp. 19-34). Routledge.

Rosano, A. (2016). Protecting Europe beyond its Borders: The Agreements between Europol and Third States or International Organizations. *Cadernos de Dereito Actual*, *4*, 9-21.

Schinina, M. (2020). What balance between Eurojust and Europol from a parliamentary angle?. *New Journal of European Criminal Law*, *11*(2), 123-134.

Voss, W. G. (2021). The concept of accountability in the context of the evolving role of ENISA in data protection, ePrivacy and cybersecurity. In *Technocracy and the Law* (pp. 246-284). Routledge.