Europol: An Overwhelming Stream of Big Data

Hoek, D.B.C.; Stigter, J.; Vermeulen, G.; Bellaert, W.

Vol. 92 issue 2, 2021

RIDP

Gert Vermeulen,
Wannes Bellaert *(Eds.)*

EU Criminal Policy: Advances and Challenges

Revue Internationale de Droit Pénal
International Review of Penal Law
Revista internacional de Derecho Penal
Международное обозрение уголовного права
刑事法律国际评论
المجلة الدولية للقانون الجنائي
Revista Internacional de Direito Penal
Rivista internazionale di diritto penale
Internationale Revue für Strafrecht

IRCP

MAKLU

AIDP – Association Internationale de Droit Pénal | The International Association of Penal Law is the oldest association of specialists in penal law in the world. Since 1924, it is dedicated to the scientific study of criminal law and covers: (1) criminal policy and codification of penal law, (2) comparative criminal law, (3) international criminal law (incl. specialization in international criminal justice) and (4) human rights in the administration of criminal justice. The Association's website provides further information (http://www.penal.org).

RIDP – Revue Internationale de Droit Pénal | The International Review of Penal Law is the primary publication medium and core scientific output of the Association. It seeks to contribute to the development of ideas, knowledge, and practices in the field of penal sciences. Combining international and comparative perspectives, the RIDP covers criminal law theory and philosophy, general principles of criminal law, special criminal law, criminal procedure, and international criminal law. The RIDP is published twice a year. Typically, issues are linked to the Association's core scientific activities, i.e. the AIDP conferences, Young Penalist conferences, world conferences or, every five years, the International Congress of Penal Law. Occasionally, issues will be dedicated to a single, topical scientific theme, validated by the Scientific Committee of the Association, comprising high-quality papers which have been either presented and discussed in small-scale expert colloquia or selected following an open call for papers. The RIDP is published in English only.

Peer review: All contributions are subject to double-layered peer review. The primary scientific and peer review responsibility for all issues lies with the designated Scientific Editor(s). The additional scientific quality control is carried out by the Executive Committee of the Editorial Board, which may turn to the Committee of Reviewers for supplementary peer review.

ISSN – 0223-5404
ISBN 978-90-466-1134-0
D/2022/1997/1
NUR 824
BISAC LAW026000
Theme: LNF, LAR

Maklu- Publishers
Somersstraat 13/15, 2018 Antwerpen, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com, www.isbs.com

Editorial Board

Summary

EUROPOL: AN OVERWHELMING STREAM OF BIG DATA

By Dante Hoek[*] and Jill Stigter[**]

Abstract

After the Paris terrorist attacks the French authorities provided Europol with 16,7 terrabytes of data. The data included information on persons falling outside of the scope of Europol's mandate. Notwithstanding, Europol started processing the data in order to identify linkages to persons formerly unrelated to crime. In a 2020 decision, the European Data Protection Supervisor (EDPS) admonished Europol for this data processing practice. In response, the European Commission proposed to legitimise Europol's Big Data processing by amending the Europol Regulation. In the run up to an agreement between the co-legislators on the new Regulation, the EDPS issued a deletion order to Europol for its incompatible data files. This paper analyses the (proposal for the) new 2022 Europol Regulation as regards Big Data processing.

1 Introduction

The utilisation of data in sciences, businesses and governments has a long history. However, the production and nature of data have transformed radically, as the amount of data humanity creates, captures and consumes worldwide has increased rapidly.[1] In 2010, the total worldwide volume of information was two zettabytes[2], whereas this year it is estimated that we will reach 74 zettabytes, which in turn is forecast to double in 2024.[3] Rather than being scarce and limited in access, data production is increasingly becoming a 'deluge' that has transformed the way government agencies and other actors operate.[4] Consequently, we are in the midst of what professor Kitchin calls 'the Data Revolution'.[5]

[*] International Master Programme in Advanced Research in Criminology (IMARC). For correspondence: <dantehoek@hotmail.nl>.

[**] Rapporteur and intern with the Border Violence Monitoring Network; International Master Programme in Advanced Research in Criminology (IMARC). For correspondence: <jillstigter@gmail.com.

[1] 'Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024' (*Statistica, 7 June 2021)* <https://statista.com/statistics/871513/worldwide-data-created/> accessed 26 March 2021.

[2] A zettabyte is equivalent to 1,000,000,000,000,000,000,000 [10^{21}] bytes or approximately a trillion gigabytes.

[3] Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024 (*Statistica, 7 June 2021)* <https://statista.com/statistics/871513/worldwide-data-created/> accessed 26 March 2021.

[4] Rob Kitchin, 'Big data, new epistemologies and paradigm shifts', [2014] volume 1 issue 1 *Big Data & Society, < https://journals.sagepub.com/doi/pdf/10.1177/2053951714528481* > accessed 19 March 2021; Wytske Van der Wagen, J. Oerlemans and Marleen Weulen Kranenberg (eds), *Basisboek cybercrime. Een criminologisch overzicht voor studie en praktijk*, 1st ed, Boom Lemma 2020, 49.

[5] Rob Kitchin, 'Big data, new epistemologies and paradigm shifts', [2014] volume 1 issue 1 *Big Data & Society, < https://journals.sagepub.com/doi/pdf/10.1177/2053951714528481* > accessed 19 March 2021;

The President of the European Commission, Ursula von der Leyen, has made digitalization a political priority for the legislative period of 2019-2024, as she aims to create 'a Europe fit for the digital age'.[6] One of the focus points is to present a new European Data Strategy that will enable the EU to 'make the most of the enormous value of non-personal data as an ever-expanding and reusable asset in the digital economy'.[7] According to the Commission, a key asset to making the best possible use of the available digital data is Big Data analytics.[8] Additionally, addressing the security aspect of the advancing digitalization should be one of the focus points, as with the digital growth the 'attack surface and potential for manipulation or criminal and terrorist abuse' also continues to increase.[9] Europol, the European Union Agency for Law Enforcement Cooperation, could play a significant role in addressing this security aspect. The agency is already equipped to make use of Big Data analytics, but Commissioner Johansson emphasised in her speech in February 2021 that the processing of large datasets was not sufficiently foreseen by the current Europol mandate.[10] Thus, during her speech before the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), she proposed the amendment of the 2016 Europol Regulation.[11] The proposal addresses a 'massive expansion' of the scope of Europol's data-gathering powers to counter the 'big data challenge' Europol is supposedly experiencing.[12] This paper draws on the initial Commission proposal (December 2020), the discussions in the Council of the EU (started in January 2021), the European Parliament (discussing a draft report in the LIBE Committee end of May 2021) and in the trilogues,[13] and the agreed text of the new Regulation. Political agreement at trilogue level was reached on 1 February 2022, with formal approval by the European

[6] Commission, 'Commission Work programme 2020' COM(2020) 37 final.

[7] Ibid.

[8] The European Commission, 'Shaping Europe's digital future: Big Data' (*digital strategy* 9 March 2021), <https://digital-strategy.ec.europa.eu/en/policies/big-data> accessed on 26 March 2021.

[9] Franca Köning 'Big Data, 5G and AI: How Europol could help Von der Leyen achieve her goals' (Hertie School: Jacques Delors Centre 2020)

[10] Commissioner Johansson 'speech'(Committee on Civil Liberties, Justice and Home Affairs, Brussel, 24 February 2021) <Commissioner Johansson's speech before the Committee on Civil Liberties, Justice and Home Affairs on the Europol mandate | European Commission (europa.eu)> accessed 1 December 2021; European Data Protection Supervisor Decision relating to European Data Protection Supervisor's own initiative inquiry on Europol's big data challenge [2020].

[11] European Parliament and Council Regulation (EU) 2016/794 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 [2016] OJ L135/53.

[12] 'Widening the net: massive expansion of Europol's data-gathering powers proposed' (Statewatch 23 February 2021) <https://www.statewatch.org/news/2021/february/widening-the-net-massive-expansion-of-eurpol-s-data-gathering-powers-proposed/, accessed 4 April 2021; Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final.

[13] European Parliament Legislative Observatory, '2020/0349(COD) Strengthening Europol's mandate: cooperation with private parties, processing of personal data, and support for research and innovation' (*Legislative Observatory* 1 December 2021) < Procedure File: 2020/0349(COD) | Legislative Observatory | European Parliament (europa.eu)> accessed 1 December 2021.

Parliament and the Council on 4 respectively 24 May 2022. The text should be published in the Official Journal and enter into force before the end of June 2022.

Considering the ensuing alteration of Europol's current operational legal basis, this papere analyses how Europol manages Big Data analytics by critically assessing the Commission's proposed revision of the 2016 Europol Regulation and Europol's practices from an EU policy perspective. The purpose is to contribute to the debate regarding Europol's mandate and to further discuss the balance between data protection, privacy, and security within the EU.

This paper sketches the European context of Big Data (analytics) and its relevance for Europol, before setting out its pre-2022 legal framework. Subsequently, the criticism provided by the European Data Protection Supervisor and Europol's Action Plan are analysed. Finally, the (proposal for the) new Europol Regulation is reviewed, and a general conclusion presented.

2 Big Data Analytics in a European Context

2.1 Europol's Big Data background

The academic literature describes how the term 'Big Data' is relatively difficult to define, and consequently, a commonly accepted definition remains absent.[14] Nevertheless, certain authors describe how Big Data refers to data of people (or objects) that are stored automatically and available for analysis in order to retrieve underlying patterns.[15] Similarly, Article 29 of the Data Protection Working Party defines Big Data as 'gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms'.[16] The difficulty in determining when a collection of data can be seen as 'Big Data', lies in the time period: what is considered Big Data in 2010 might not correspond with the 'bigness' of data in 2021.[17] Consequently, some authors determine how Big Data is a 'made-up catchword' or an 'um-

[14] Isitor Emmanual and Clare Stanier 'Defining big data' in Djallel Eddine Boubiche, Hani Hamdan and Ahcène Bounceur, *BDAW'16Proceedings of the International Conference on Big Data and Advanced Wireless Technologies* (Association for Computing Machinery, 2016).

[15] Judtih van Erp, Wouter Stol and Johan van Wilsem 'Criminaliteit en criminologie in een gedigitaliseerde wereld' [2013] 55 (4) Tijdschrift voor Criminologie, 327.

[16] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation [2012].

[17] Paul De Hert and Vagelis Papakonstantinou, 'Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms' [2021] 40 Computer Law & Security Review; Isitor Emmanual and Clare Stanier 'Defining big data' in Djallel Eddine Boubiche, Hani Hamdan and Ahcène Bounceur, *BDAW'16Proceedings of the International Conference on Big Data and Advanced Wireless Technologies* (Association for Computing Machinery, 2016).

brella term', and therefore, serves as an expression for the technological capacity to process larger volumes of data.[18] In practice, it means that Big Data cannot be processed by Europol with regular tools, but 'require specific tools and storage facilities'.[19]

Big Data only became a 'main topic of discussion' in European policymaking after 2015 across many areas, such as 'scientific and technological research, law enforcement, national security, government transparency as well as open-source information and intelligence'.[20] This can be traced back to a decision on 20 November 2015 by the EU Justice and Home Affairs Ministers to establish a European Counter Terrorism Centre (ECTC) at Europol.[21] The ECTC was set up to provide operational and analytical support to the authorities of the Member States in the context of the fight against terrorism.[22] The decision was made after the Paris attacks on 13 November 2015 after which the establishment of the ECTC was seen as 'a major strategic opportunity for the EU to make our collective efforts to fight terrorism more effective'.[23] The ECTC would operate within the already existing framework of Europol and its organisational structure. The Centre's end goal was to maximise the exchange capabilities in operational, technical, and general information regarding counter-terrorism initiatives.[24] An example of ECTC's added value through cooperation and support were the 'unprecedented levels of information (of over 16,7 terabytes)' that were shared and analysed, and phone data analysis that were conducted after the Paris attacks.[25] Additional to the counter-terrorism initiatives, Europol provides insight into the threat and development of serious and organised crime (e.g., cybercrime, trafficking in human beings, and drug production, trafficking and distribution) in the Serious and Organised Crime Threat Assessment (SOCTA) to the EU's decision-makers and law enforcement community.[26] For the SOCTA of 2017, Europol had 'undertaken the largest-ever data collection on serious and organised crime in the EU'

---

[18] Ibid.

[19] European Parliament Legislative Observatory, '2020/0349(COD) Strengthening Europol's mandate: cooperation with private parties, processing of personal data, and support for research and innovation' (*Legislative Observatory* 1 December 2021) < Procedure File: 2020/0349(COD) | Legislative Observatory | European Parliament (europa.eu)> accessed 1 December 2021.

[20] Daniel Drewer and Vesela Miladinova 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) Computer Law & Security Review, 298 – 308 p.

[21] Council conclusion 14419/15 Press release 845/15 on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism [2015] <www.consilium.europa.eu/en/press/press-releases/2015/11/20/conclusions-radicalisation/> accessed 21 March 2021.

[22] Council Note 9201/16 on Information sharing in the counter-terrorism context: Use of Europol and Eurojust [2016] < eu-council-c-t-info-sharing-9201-16.pdf (statewatch.org)> accessed 21 March 2021.

[23] 'Europol's European Counter Terrorism Centre strengthens the EU's response to terror' (*Statewatch, 2016*) <Europol's European Counter Terrorism Centre strengthens the EU's response to terror (statewatch.org)> accessed 3 April 2021.

[24] Daniel Drewer and Jan Ellerman, 'May the (well-balanced) force be with us! The launch of the European Counter Terrorism Centre (ECTC)' [2016] 32(2) *Computer Law & Security Review*, 195.

[25] Council Note 9201/16.

[26] Europol, 'Serious and Organised Crime Threat Assessment (SOCTA): Identifying the priorities in the fight against major crime' <https://europol.europa.eu/socta-report> accessed 3 April 2021.

where they received large contributions from the Member States, partners outside the EU, the institutional partners and information provided by Europol's own databases.[27]

Shortly after the decision of the EU Justice and Home Affairs Ministers on the establishment of the ECTC, an agreement was reached between members of the European Commission, the Council, and the Parliament on a consolidated draft of the Europol Regulation which applies from 1 May 2017.[28] The then-brand-new Regulation incorporated a 'flexible and modern integrated data management system' that would improve and modernise the framework regarding information sharing and create new opportunities for technological advancements in the field of criminal investigations.[29] This shift from traditional to more technologically advanced instruments to combat terrorism and organised crime required a similar shift of traditional meanings of privacy and information-sharing methods.[30] Since 2016, several legal instruments have been adopted that lay down more general data protection rules in the European Union: the Law Enforcement Directive[31] and the Regulation establishing data protection rules for the bodies of the European Union (EUDPR)[32]. The legal basis for reforms on the protection of personal data is laid down in the Treaty on the Functioning of the European Union.[33] Even though data protection and privacy are both fiercely protected fundamental rights within Europe, there is a certain discretionary power given to the Member States, judicial bodies and law enforcement agencies (e.g., Europol) to determine the demarcations of the abovementioned fundamental rights regarding the ever-evolving digitalisation.[34] Ultimately, the most important thing is striking a balance between privacy and data protection, on the one hand, and general interests like public and national security, on the other.[35]

---

[27] Europol, 'European Union Serious and Organised Crime Assessment (SOCTA)' [2017].

[28] Regulation (EU) 2016/794.

[29] Daniel Drewer and Vesela Miladinova 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) *Computer Law & Security Review*, 298 – 308 p.

[30] Ibid.

[31] European Parliament and Council Directive 2016/680 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 of the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/81.

[32] European Parliament and Council Regulation 2018/1725 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 45/2001/EC and Decision 1247/2002/EC [2018] OJ L295/39.

[33] Consolidated version of the Treaty on the Functioning of the European Union, *OJ C 326/01*, Article 16.

[34] EDPS Background paper, 'Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights' [2017]; EDPS Report, 'The EDPS Strategy 2015-2019' [2015].

[35] Daniel Drewer and Vesela Miladinova 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) Computer Law & Security Review, 298 – 308.

2.2 CJEU and Big Data processing

The search for the right balance remains a point of discussion, as some authors point to how 'we complain when they [security agencies] don't keep us safe. And we complain when they [security agencies] snoop illegally into our data in order to keep us safe'.[36] This leaves us with the question of where the current balance lies between these two complaints.[37] When it concerns national security, the Court of Justice of the European Union (CJEU) has aimed to clarify to what extent the collection and retention of bulk data for national security purposes is possible in three combined cases, of which one is *La Quadrature du net and Others v. Premier Ministre*.[38] More specifically, *La Quadrature du Net* concerns the retention of communication data[39] in a general or indiscriminate way for national security purposes and questions whether these practices are compatible with EU law.[40] According to the CJEU, the Member States are allowed under certain conditions to collect and retain large amounts of data for national security purposes, such as terrorism. The Member States can afterwards provide the retained information to Europol for their operational Big Data analyses. Over the past years, Europol has been receiving increasing amounts of data, such as the previously mentioned 16,7 terabytes that were shared after the Paris attacks.[41] The EU institutions are more inclined to take on a narrower perspective in order to enhance their role in national security matters.[42] Nonetheless, the GDPR explicitly mentions that it does not apply to data protection related to national security, because it falls outside of EU law.[43]

On the one hand, the Court confirms this by stating that national security concerns do not exclude the Member States from the need to comply with general principles of EU law such as proportionality and respect for fundamental rights like privacy, data protection and freedom of expression.[44] This ruling could therefore have limited the Member States in their ability to forward large and indiscriminate datasets to Europol for processing. Consequently, the agency could receive less information than in the past. On the

---

[36] Jonathan Goldsmith, 'CJEU decides against UK government on data protection' (2020) (<www.lawgazette.co.uk/commentary-and-opinion/cjeu-decides-against-uk-government-on-data-protection/5105963.article> accessed 10 April 2021)

[37] Ibid.

[38] Case C-511/18 La Quadrature du Net and Others v. Premier minister [2020].

[39] Communication data is information about who is communicating with whom, when, and where. This can still be considered sensitive information as it exposes details about the personal life of an individual. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Minister for Communication and Others, C-293/12; C-594/12, ECLI:EU:C:2014:238, para 39: 'traffic and location data, aggregated and taken as a whole, could be analysed and depict a detailed picture of individuals' private lives.'

[40] Monika Zalnieriute, 'The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments' [2020] 24(28) American Society of International law.

[41] Council Note 9201/16.

[42] Ibid.

[43] Regulation 2016/679, Recital 16.

[44] La Quadrature du Net and Others v. Premier minister, para 113.

other hand, the Court explains how 'genuine and present or foreseeable' national security threats can form an exception, and justify data collection and retention[45], as long as this decision is reviewed by a court or an independent administrative body[46]. Yet, these practices have to be limited to 'what is strictly necessary'.[47] Hereby, in an attempt to demarcate and limit the possibilities of Big Data processing for national security purposes, the CJEU simultaneously provided an exception, which can be seen as newly opened doors for security agencies. In particular, regarding the meaning of how much data is 'strictly necessary' in a national security context, it is likely that the definition of government agencies will differ from the definition of civil rights advocacy groups.[48] Changing views on national security by the Member States could be the consequence, which will then again result in cases before CJEU to unfold the struggle or make it worse. At the same time, it should be emphasized that the CJEU's exception is only applicable when combatting 'serious crime' and only possible when conditions and limitations are met. In addition, the Court notes how access to the data retained for legitimate or national security purposes 'may in no event be granted'.[49] Thereby, *La Quadrature du Net* is a complex judgement. At first sight, the Court offers a positive confirmation of data protection and privacy, but after a closer look, its decision to legitimise indiscriminate data retention in certain circumstances is also in sharp contrast with the strict post-Snowden data protection approach.[50]

2.3 Relevance and challenges of Big Data analytics for Europol

The key opportunity for Big Data is: 'the availability of new sources of dynamic, resolute data that can potentially complement, replace, improve, and add to existing datasets and refine existing statistical composition, and produce more timely outputs'.[51] For Europol, the relevance of big data is related to several areas, 'particularly cybercrime, terrorism-related propaganda, enhanced risk entities solution (ERES), open-source information (OSINF) and open-source intelligence (OSINT)'.[52] In addition, information sharing on counter-terrorism and organised crime are both very high on the agenda of the Member

[45] Ibid, para 137.
[46] Ibid, para 139.
[47] Ibid, para 132.
[48] Natasha Lomas, 'Europe's top court confirms no mass surveillance without legal limits' (2020) (<Europe's top court confirms no mass surveillance without limits | TechCrunch> accessed 10 April 2021.
[49] La Quadrature du Net and Others v. Premier minister, para 166.
[50] Monika Zalnieriute, 'The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments' [2020] 24(28) American Society of International law ('[...] in its most recent ruling in Schrems II case, delivered just two months earlier, on July 16, 2020 [...] the CJEU invalidated the EU-US Privacy Shield agreement for lack of safeguards in the national surveillance system of the US.').
[51] Rob Kitchin, 'The opportunities, challenges and risks of big data for official statistics' [2015] 31(3) Statistical Journal of the IAOS, 472.
[52] Daniel Drewer and Vesela Miladinova 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) Computer Law & Security Review, 298 – 308.

States and the EU.[53] This is reflected through the high increase in the amount of information that is exchanged, even though the usage of systems, tools and services provided by the EU varies greatly between the Member States. Being able to process bigger datasets would make it possible for Europol to increase its profiling successes.[54] It is argued by the European Commission how Europol, in contrast to the Member States, is capable of detecting cross-border links in the analysis of larger datasets. In other words, the datasets at the national level 'lack the corresponding data on other crimes and criminals in other Member States'.[55] Moreover, it is possible that certain Member States do not have the means to run Big Data analysis, as IT tools, expertise and resources are necessary to run complex datasets.[56] Europol actively cooperates with law enforcement authorities of Member States and has been able to establish valuable links between crimes and identify new lines of investigation. For example, after the terrorist attacks in France, Europol set up the Task Force *Fraternité* in 2016 which started analysing Big Data with a software program called 'Gotham'.[57] Since mid-2017, however, the operational analysis of all counter terrorism-related data uses this software.[58] Gotham enables investigators to calculate and visualise relationships between persons, objects or the course of events.[59] The results from the analyses help to identify new investigative hints that are used by the competent authorities in EU Member States.[60]

At the same time, it is of importance to note that the use of Big Data analytics for law enforcement purposes does not only present opportunities but also various challenges. The predictive power of Big Data analytics cannot be taken for granted as biases and limitations come into play when used in decision-making. In particular, the output of the analyses is not objective as the data can be provided by different sources and collected with different methods.[61] When unreliable information is used or relevant information is lacking, errors or gaps in the results are present. This limitation relates to certain characteristics of Big Data, such as veracity and value, as the quality of data relies on a considerable amount of interpretation which is inevitably subjective. When larger amounts of

---

[53] Europol, 'Exploring tomorrow's organised crime' [2015]; Europol, 'Internet Organised Crime Threat Assessment (IOCTA)' [2020].

[54] Daniel Drewer and Vesela Miladinova 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) Computer Law & Security Review, 298 – 308.

[55] Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final 6.

[56] Ibid.

[57] European Commission, 'Palantir software at EU agencies' E-000173/2020(ASW).

[58] Ibid.

[59] Matthias Monroy, 'Europol uses Palantir' (2020) (<https://digit.site36.net/2020/06/11/europol-uses-palantir/> accessed 26 March 2021).

[60] Ibid.

[61] Alexander Babuta, Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities (Royal United Services Institute for Defence and Security Studies: Occasional Papers 2017), 1 – 54.

data from different sources are processed, it is not only the potential for error that increases but also the possibility of detecting false positive relationships.[62] This could result in misinterpretation, bias, and discrimination in the decision-making process. Therefore, when applying Big Data analytics in practice, the wider operational, organisational, and legal context must be carefully considered in order to prevent bias and ensure effectiveness.[63] In other words, the aim is to create discriminatory policing practices in a non-discriminatory fashion. Nevertheless, concerns about the presence of bias in Big Data processing by Europol are present and have been addressed during the European Parliament debate on 24 February 2021, when a Member of the European Parliament (MEP) Clare Daly responded to the speech by Commissioner Johansson on the extension of Europol's mandate.[64] In particular, she stated: 'I think this will be actually a good time to look at […] how racism and discrimination can feed up the chain of Europol because the agencies' work rests on the information it gets from the Member States'.[65] The criticism is valid as evidence of racist and discriminatory policing practices in the Member States has been provided.[66] Consequently, as Europol's actions, in turn, affect national law enforcement activities, possible unjustifiable negative effects on the lives of certain groups of individuals could be the result. Hereby, another layer of complexity is added to Europol's already demanding Big Data challenge.

3 Legal Framework for (Big) Data Processing by Europol

3.1 Europol Regulation

The 2016 Europol Regulation provided the agency with the appropriate tools for 'modernisation, but also adaptation to the shifting *modus operandi* of terrorism and serious and organised crime'.[67] The Regulation contained a 'reinforced robust data protection regime' that was 'based on an innovative privacy by design approach', namely the Integrated Data Management Concept (IDMC).[68] The approach introduced the concept of 'interoperability' for Europol where one dataset could be combined and analysed with another dataset without it causing procedural issues. For Europol, this meant more flexibility when information and personal data would be processed.[69]

---

[62] Ibid.

[63] Alexander Babuta and Marion Oswald, 'Data analytics and algorithmic bias in policing' (2019) Royal United Services Institute for Defence and Security Studies: Briefing Papers (<RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf (publishing.service.gov.uk)> accessed 23 March 2021.

[64] Clare Daly (MEP) Remark, Brussel (Europol mandate), 24 February 2021.

[65] Ibid.

[66] Dietrich Oberwittler and Sebastian Roché, Police citizen relations around the world. Comparing sources and contexts of trust and legitimacy (1st ed, Routledge, 2019).

[67] Daniel Drewer and Vesela Miladinova 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) Computer Law & Security Review, 298 – 308.

[68] Ibid.

[69] Ibid.

Several concepts have been specifically defined in the Regulation, namely the sources[70] and purposes of information[71], categories of personal data to be collected[72], categories of data subjects[73], and finally, the access rights to information[74]. Under the Regulation, Europol is allowed to potentially use large quantities of data in cases of a strategic nature and if there are adequate data protection safeguards put in place.[75] Currently, Europol is only allowed to process data on the following categories of data subjects: suspects, potential future criminals, contacts and associates, victims, witnesses, and informants.[76] Additionally, the Regulation further defines several categories of personal data Europol is allowed to process on the abovementioned categories of data subjects, such as personal details, contacts and associates, information relating to criminal conduct, victim identification data, et cetera.[77] In order to limit the access of the Member States to the large amounts of data that are gathered and used by Europol, there are several safeguards put in place.[78] Big Data analytics is only to be used for the purpose of strategic analyses as an additional way to support policy decisions or preventing criminal actions like terrorism or serious organised crime.[79] The broad scope of the provision on the processing of personal data for the purpose of strategic analysis reflects the many different forms of data that are allowed to be collected.[80] Additionally, these processing operations of personal data need to be documented by Europol and made available to the Data Protection Officer and the European Data Protection Supervisor.[81] In particular, Article 30(2) of the Europol Regulation can be seen as an initiative to enforce appropriate safeguards for data protection, as it states how the '[p]rocessing of [sensitive personal data], by automated or other means, shall be prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives'. More importantly, the Regulation stipulates how 'no decision by a competent authority which produces adverse legal effects, shall be based solely on automated processing'.[82] The latter ensures how human intervention is always present which relates back to the prevention of possible biases present in Big Data analytics, as discussed earlier.

[70] Regulation (EU) 2016/794, Article 17.
[71] Ibid, Article 18.
[72] Ibid, Article 18(5) and Annex II.
[73] Ibid.
[74] Ibid, Article 20.
[75] Ibid, Article 18(4).
[76] Ibid, Annex II B(1)
[77] Ibid, Annex II B(2)(3)(4)(5)(6).
[78] European Parliamentary Research Service, 'Revision of the Europol Regulation' [2021].
[79] Regulation 2016.794, Article 2(b).
[80] Ibid, Article 18(4).
[81] Ibid, Article 30(2).
[82] Ibid, Article 30(4).

3.2 Data protection, supervisory bodies and the role of Council and Parliament

The Europol Regulation contains its own autonomous data protection regime, even though there is a subsequently adopted Regulation on the protection of individuals regarding the processing of personal data by the Union institutions, bodies, offices and agencies (EUDPR).[83] The EUDPR currently does not apply to Europol, though the Commission is obliged to review this before April 2022.[84] The Europol Regulation does provide individuals with the right to ask for information on the processing of data relating to them[85], the right to ask for rectification, erasure and restriction of such data[86], and the right for their data to be processed following the data protection principles[87].

In terms of oversight, supervision on the application of the data protection safeguards by Europol is conducted throughout the entire information cycle.[88] On a national level, Europol is supervised by the competent national authorities under the applicable national law.[89] This national supervisory authority will check the permissibility of the 'transfer, retrieval and communication to Europol of personal data by the Member State concerned' and examines whether this 'violates the rights of the data subjects concerned'.[90] Internally, the Member States and European Commission are represented within Europol in the Management Board.[91] Among its tasks, the Management Board appoints an independent Data Protection Officer (DPO).[92] The DPO is tasked with ensuring the lawful application of the Europol Regulation regarding processing personal data, ensuring that a record is kept of said processing of personal data, and ensuring that at the request of data subjects they are informed of their individual rights.[93] Furthermore, the DPO prepares an annual report, registers breaches of personal data, and has close cooperation with Europol staff and the European Data Protection Supervisor (EDPS).[94] The EDPS has the responsibility to ensure and monitor the 'protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by

[83] Regulation (EU) 2018/1725.
[84] Ibid, Article 98.
[85] Regulation (EU) 2016/794, Article 36.
[86] Ibid, Article 37.
[87] Ibid, Article 28.
[88] Daniel Drewer and Jan Ellerman, 'Europol's data protection framework as an asset in the fight against cybercrime' [2012] 13(3) *ERA Forum* 381 – 395.
[89] Regulation (EU) 2016/794, Article 42.
[90] Ibid, Article 42(1).
[91] Ibid, Article 10(1)
[92] Ibid, Article 11(1)(I) and 41(1).
[93] Ibid, Article 41(6)(a)(b)(c)
[94] Regulation (EU) 2016/794, Article 41(6)(d-g).

Europol'.[95] Additionally, they have the authority to warn or admonish Europol[96], which they officially did in September 2020 on the processing of Big Data by Europol[97].

When it comes to the European Parliament, they can put in a request to gain access to 'sensitive non-classified information processed by or through Europol' to exercise parliamentary scrutiny.[98] However, according to the European Parliamentary Research Service (EPRS), 'parliamentary scrutiny over Europol remains rather limited'.[99] As mentioned before, only the Commission and the Member States are represented within Europol's Management Board, without any involvement of the Parliament.[100] The appointment of the Executive Director goes through the Council of the European Union on the basis of a proposal issued by Europol's Management Board.[101] In this case, the European Parliament *may* issue a non-binding opinion on the candidate after they have been invited to and appeared before the Parliament.[102] However, Europol's activities are monitored and evaluated by members of the European Parliament's LIBE Committee together with the national parliaments under a specialised Joint Parliamentary Scrutiny Group (JPSG).[103] The JPSG can request the Executive Director and the Chairperson of the Management Board to appear before them to discuss matters related to their activities in 'fulfilling its mission' and the impact of these activities on 'the fundamental rights and freedoms of natural persons'.[104] Through this, the European Parliament can hold both the Executive Director and the Management Board accountable regarding 'the management of the agency'.[105] It may be true that, according to the EPRS, the European Parliament does not have 'any particular real powers' if we follow the wording of the provisions of the Europol Regulation.[106] However, that does not mean that they should have stronger powers in that regard, as this might blur the controlling function the Parliament has. The suggestion by the EPRS, for example, to include an observer from the European Parliament in Europol's Management Board as to have 'more information and more awareness of what the agency is doing'[107], is one solution that still fits within the Parliament's controlling function and does not provide them with more power just for the sake of having

[95] Ibid, Article 43(1).
[96] Ibid, Article 43(3)(d).
[97] EDPS Decision, 'European data Protection Supervisor's own initiative inquiry on Europol's big data challenge' [2020].
[98] Regulation (EU) 2016/794, Article 52(1).
[99] European Parliamentary Research Service, *EU agencies common approach and parliamentary scrutiny*, November 2018.
[100] Ibid.
[101] Regulation (EU) 2016/794, Article 54(2).
[102] Ibid.
[103] Ibid, Article 51(1).
[104] Ibid, Article 51(2)(a)
[105] European Parliamentary Research Service, 'EU agencies common approach and parliamentary scrutiny' [2018].
[106] Ibid.
[107] Ibid.

more power. Within the context of the Proposal for renewal of Europol's mandate, however, it is necessary that an evaluation of the JPSG's work is conducted to indicate if the group 'has been able to carry out its tasks effectively and how its role might be extended to ensure more regular and effective democratic scrutiny'.[108]

4 EDPS Criticism and Europol's Response

4.1 EDPS Decision

In September 2020, the EPDS published an official warning about Europol's Big Data processing practices, despite the restrictions and safeguards present in the Europol Regulation.[109] In the Decision, Supervisor Wiewiórowski describes how there is a 'high likelihood that Europol continually processes personal data on individuals for whom it is not allowed to do so' and therefore is breaking its own data protection rules.[110] The issue concerns an enormous database that stored more than two million gigabytes, provided by the Member States to Europol for processing. As a result, large amounts of personal data are stored in Europol's systems for several years which 'undermines the principle of data minimisation'.[111] The admonishment by the EDPS cannot be taken lightly as fundamental rights and freedoms of data subjects are at risk.[112] More importantly, they could be wrongfully linked to criminal activity in the European Union.[113] The EDPS indicated that in order for the prevention of any damage to the personal and family life, free movement and occupation of data subjects, there needs to be a proper implementation of the data minimisation principle and safeguards that are included in the Europol Regulation.[114] At the same time, the EDPS acknowledges how the volume of data was 'simply too big' to ascertain that all the information would comply with the data protection rules. So, the Big Data sets provided by the Member States were beyond the technical capability of Europol. Finally, the EDPS notes how finding a solution could be a challenge, as the 'legal concerns identified [are] structural as they relate to Europol's core working methods'[115]. In other words, the Decision of the EDPS addresses both technical and ethical issues regarding the processing of large datasets by Europol and shows how Europol has been illegally processing large amounts of certain data. MEP Patrick Breyer commented

[108] 'Submission to the European Commission's consultation on revising Europol's mandate' (*Statewatch, 8 July 2020*) < eu-europol-consultation-submission-8-7-20.pdf (statewatch.org)> accessed 22 August 2021.
[109] EDPS Decision, 'European data Protection Supervisor's own initiative inquiry on Europol's big data challenge' [2020].
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] Ibid.
[114] Ibid.
[115] Ibid.

on the EDPS report by rightfully saying: 'It's clearly illegal to retain data on non-suspects'.[116] Europol is required to address the criticism in an Action Plan, which is presented in the next section.

4.2 Europol's Action Plan

In response to the Decision of the EDPS, Europol was tasked with devising a plan of action that addresses and mitigates the data protection concerns put forward. The agency states in this Action Plan how the 'legal concerns' of the EDPS provide an opportunity to not only ensure that Europol complies with its legal mandate in the future, but also can ensure their ability to 'provide operational support to EU member states in their fight against serious crime and terrorism.'[117] Consequently, Europol expresses support for the amendment of its legal basis as reflected in the Commission's proposed revision of the 2016 Europol Regulation which will be discussed in more detail later. More specifically, Europol states how similar breaches should be prevented in the future through the proposed revision of their mandate as it provides a stronger legal basis for handling large datasets.[118] In other words, Europol has mostly defended its current practice of using large datasets for criminal investigations by supporting the proposal that allows the agency to continue its practices.

At the same time, the Action Plan presents concrete measures that should prevent the processing of data beyond its scope. In particular, Europol focuses in the Action Plan on two aspects: 1) reducing the risks for data subjects by ensuring an enhanced data review, and 2) building a new technical platform for handling large datasets.[119] Therefore, Europol aims to enhance both information security principles and data protection controls. In particular, the aim is to strengthen data review arrangements before an analysis is performed, specifically by flagging in Europol's data environment.[120] The flagging serves as a sign to staff that not all data has been determined to be in line with the categories listed in Annex II of the Europol Regulation[121], which should 'mitigate' the risk that data is further processed.[122] Moreover, Europol aims to limit the number of persons who have

---

[116] Vincent Manancourt and Zosia Wanat, 'EU regular warns Europol could be breaking data rules', *Politico* (20 October 2020) <www.politico.eu/article/eu-regulator-warns-europol-could-be-breaking-data-rules/> accessed on 26 March 2021.

[117] Europol, 'Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge' [2020].

[118] Council Resolution 12463/20 on the Future of Europol [2020].

[119] Europol Document, 'Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge' [2020].

[120] Ibid.

[121] Regulation (EU) 2016/794, Annex II B(1) limits the categories of data subjects about whom Europol can process to suspects, potential future criminals, contacts and associates, victims, witnesses and informants. Annex II B(2), (3), (4), (5) and (6) define which categories of personal data Europol can process in relation to each of the categories of data subjects.

[122] EDPS Decision, 'European data Protection Supervisor's own initiative inquiry on Europol's big data challenge' [2020].

access and are allowed to assess the data, whilst appointing a Data Quality Control Coordinator to ensure that 'data processing is performed in line with the Europol Regulation'.[123]

4.3 Assessment of Europol's response to the EDPS Decision

While the Action Plan of Europol presents several relevant measures, it remains relatively tangible, as the underlying premise continues to be the extension of its legal scope which would ensure that the extensive data processing the agency was accused of, would be allowed under a new legal framework. The measures presented in the Action Plan aim to 'mitigate' the risks that unlawful data is processed, which cannot be deemed sufficient, as these risks relate to a breach of the fundamental rights of citizens.[124] Therefore, these risks ought to be reduced as much and as soon as possible; especially since, according to the EDPS, the risks relate to a structural working method.[125] In addition, not only are Europol's actions considered outside their legal scope, but the Action Plan also does not call for the intermediate abolishment of their current data processing practices. In other words, Europol is currently still operating and processing extreme amounts of information without the necessary legal basis to do so. Consequently, criticism can be given regarding Europol's efforts to adequately address the admonishment of the EDPS instead of leaving the issue to be solved through a renewal for their legal framework in the future.

This matter has also been commented on by some Members of the European Parliament as they expressed their disapproval regarding the efforts the agency puts in to rectify the issue. MEP Clare Daly stated how 'the admonishment of Europol by the EDPS is extremely serious, and Europol's Action Plan in response is inadequate'.[126] In addition, Daly stated, during the Parliamentary debate on 24 February 2021, how Europol's powers have been extended more by policy decision rather than through legislation and she urges how 'we really need first to have a deep look about what Europol has been doing, otherwise we will be kind of legislating blind'.[127] So, while the recently published study conducted for the LIBE Committee notes how the official admonishment illustrates 'the

[123] Europol Document, 'Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge' [2020].
[124] Ibid.
[125] EDPS Decision, 'European data Protection Supervisor's own initiative inquiry on Europol's big data challenge' [2020].
[126] Jessie Goeman, 'Europol under fire for use of 'targeted data' tactics in criminal investigations' *NewEurope* (3 February 2021) <www.neweurope.eu/article/europol-under-fire-for-use-of-targeted-data-tactics-in-criminal-investigations/> accessed 23 April 2021.
[127] Clare Daly (MEP) Remark, Brussel (Europol mandate), 24 February 2021.

fruits' of the supervisory role of the EDPS[128], it is possible to question the existence of these 'fruits' as Europol's condoned practices are continued in practice.

5 Renewal of the Europol Regulation

5.1 Background and outline of the new Regulation

With the ever-evolving security threats, such as the terrorist attacks in France[129] and Austria[130] at the end of 2020, the European Commission put forward a proposal for a revision of the 2016 Europol Regulation.[131] Alongside the Proposal, the Commission also released (on the same day) a Communication on a Counter-Terrorism Agenda for the EU, confirming the influence of counterterrorism on Europol's reform.[132] In July 2020, Europol indicated how their current legal basis 'does not match the operational requirements and does not provide sufficient legal certainty for Europol to perform its tasks'.[133] To provide operational support to the Member States' judicial investigations and analyse information has always been at the core of Europol, or 'the DNA of Europol' and 'the reason Europol was created'.[134] In our digitalised world, the amount of data collected during criminal investigations is only increasing, which manifests itself in larger and more complex datasets given to Europol by the Member States. This ultimately resulted in the earlier mentioned 'big data challenge' for Europol, and in the admonishment by the EDPS. Nevertheless, as expressed by Europol, 'the assumption that Europol should only work on pre-sifted information containing only the information of data subject categories is not reflecting the police reality'.[135] All data that is given to Europol is collected by the Member States' judicial authorities during criminal investigations and is often unstructured. This means that it is not clear from the beginning which data is related to the data

[128] Niovi Vavoula and Valsamis Mitsilegas, 'Strengthening Europol's mandate A legal assessment of the Commission's proposal to amend the Europol Regulation' (2021) European Parliament Policy Department for Citizens' Rights and Constitutional Affairs <Strengthening Europol's mandate A legal assessment of the Commission's proposal to amend the Europol Regulation (europa.eu)> accessed 3 September 2021.

[129] 'France attack: Three killed in 'Islamist terrorist' stabbings' (*BBC NEWS*, 29 October 2020) <www.bbc.com/news/world-europe-54729957> accessed 20 April 2021.

[130] 'Vienna shooting: Austria hunts suspects after 'Islam terror' attack' (*BBC NEWS*, 3 November 2020) <www.bbc.com/news/world-europe-54788613> accessed 20 April 2021.

[131] Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final.

[132] Commission, 'a Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond' COM(2020) 695 final.

[133] Europol Document, 'Europol's main operational considerations in light of the Europol Regulation' [2020] 1.

[134] Jürgen Ebner, 'Exchange of views with Europol and EDPS on the implementation of Europol Action Plan to address the admonishment by EDPS following an own-initiative inquiry on internal big data challenges Exchange of views' (*European Parliament*, 16 June 2021) <Committee on Civil Liberties, Justice and Home Affairs - Multimedia Centre (europa.eu)> accessed 3 September 2021.

[135] Ibid.

subject categories and which data is irrelevant to the investigation.[136] The difficulty Europol experiences with selecting and processing the 'right' data has resulted in the processing of data outside of Europol's processing scope, and subsequently the extension of its processing scope in the Proposal.

Before the Proposal was put forward, the Commission initiated an Inception Impact Assessment (IIA) where they asked for feedback on the envisaged changes to the Europol Regulation.[137] In the IIA the Commission did not address the 'illegal' big data processing action undertaken by Europol, nor did it assess possible policy choices. The Commission received twenty feedback contributions in total.[138]

The eventual Proposal contained fundamental changes to the Europol mandate concerning the agency's powers and their relationship with the Member States and other parties. It addressed three main areas, namely: effective cooperation, especially with private parties, effective operational support for the Member States and their criminal investigations with analysing large datasets, and an enhanced role of the agency's role in research and innovation. A Council conclusion of December 2019 expressed that there is an 'urgent operational need for Europol to request and receive data directly from private parties' in order to ensure that 'fundamental rights such as the protection of personal data and the principles of consent […], are respected'.[139] However, even though the 'urgent operational need' was expressed by the Council, it was not based on an evaluation of the Europol mandate. In fact, neither of the central three areas in the Proposal has been based on an assessment of Europol's activities in practice. Even though, as prescribed by Article 68 of the Europol Regulation, the Commission had to ensure by 1 May 2022 'that an evaluation assessing, in particular, the impact, effectiveness and efficiency of Europol and of its working practices is carried out'.[140] This evaluation would need to address 'the possible need to modify the structure, operation, field of action and tasks of Europol'.[141] The absence of this evaluation means there exists, at the very least, the risk that no identification of any shortcomings of Europol's current mandate, or the impact and efficiency of the agency's working practices, before the proposed reforms, has taken place. In connection with this, Statewatch has expressed equal concern for the lack of a comprehensive and independent evaluation of the agency's mandate, specifically on 'how its information-processing and analysis relate to discriminatory policing practices at national

[136] Europol Document, 'Europol's main operational considerations in light of the Europol Regulation' [2020] 1.
[137] Commission, 'Staff working document - Executive summary of the Impact Assessment Report on the Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' SWD(2020) 544 final.
[138] European Parliamentary Research Service, 'Revision of the Europol Regulation' [2021].
[139] Council Conclusion 14745/19 Europol's cooperation with private parties [2019].
[140] Regulation (EU) 2016/794, Article 68(1).
[141] Ibid.

level'.[142] The problematic nature of this course of events can be illustrated by MEP Clare Daly's earlier comment as, without an evaluation, the Commission is essentially 'legislating blind'.[143]

According to the new Regulation, Europol would 'act as a technical channel for exchanges between the Member States and private parties' to prevent any problems that occurred in the past when private parties and the Member States cooperated within multiple jurisdictions within and outside of the EU.[144] Other additional changes to the Europol Regulation include strengthening the cooperation with third countries and the European Public Prosecutor's Office (EPPO), but also strengthening Europol's data protection framework and the accountability of the agency. More importantly, the new Regulation enables Europol to 'process large and complex datasets' in the context of the prevention of serious crime and terrorism.[145] In contrast to the 2016 Regulation, the new Regulation does allow the processing of personal data that do not fall under the categories named in Annex II of the Europol Regulation[146] as long as it supports an 'on-going specific criminal investigation for which the investigate data was provided'.[147] Moreover, Europol will not only be allowed to process higher volumes of data but will also be able to store the information of the investigation and the results of the analysis for as long as the criminal investigation takes.[148] These changes are prohibited under Europol's 2016 Regulation, while the new Regulation extends the ability to use Big Data analytics.[149]

In addition, the Regulation further introduces the possibility for Europol to conduct a 'pre-analysis of personal data' to determine if the gathered personal data belongs to the categories named in Annex II of the Europol Regulation.[150] This pre-analysis will take place before Europol's 'cross-checking, strategic analysis, operational analysis or exchange of information'. If the pre-analysis reveals the gathered data does not fall under

---

[142] 'Submission to the European Commission's consultation on revising Europol's mandate' (*Statewatch, 8 July 2020*) < eu-europol-consultation-submission-8-7-20.pdf (statewatch.org)> accessed 22 August 2021.
[143] Clare Daly (MEP) Remark, Brussel (Europol mandate), 24 February 2021.
[144] Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final; Recital 42 of the new Regulation
[145] Ibid.
[146] Regulation (EU) 2016/794, Annex II B(1) limits the categories of data subjects about whom Europol can process to suspects, potential future criminals, contacts and associates, victims, witnesses and informants. Annex II B(2), (3), (4), (5) and (6) define which categories of personal data Europol can process in relation to each of the categories of data subjects.
[147] Ibid, Article 18a.
[148] Ibid.
[149] 'EU: New Europol Regulation: what the agency wants, the agency gets?' (*Statewatch,* 4 Augustus 2020, <www.statewatch.org/news/2020/august/eu-new-europol-regulation-what-the-agency-wants-the-agency-gets/> accessed 16 April 2021.
[150] Regulation (EU) 2016/794, Article 18(5a). Regulation (EU) 2016/794, Annex II B(1) limits the categories of data subjects about whom Europol can process to suspects, potential future criminals, contacts and associates, victims, witnesses and informants. Annex II B(2), (3), (4), (5) and (6) define which categories of personal data Europol can process in relation to each of the categories of data subjects.

the categories of data Europol is allowed to process, this data needs to be deleted.[151] This could improve Europol's ability to categorise the gathered data and in turn, ensure the data protection principles.

5.2 Oversight and accountability mechanisms

At the same time, a stronger mandate should always be accompanied by a stronger oversight of Europol. At first glance, the new Regulation increases the parliamentary oversight and accountability of Europol by introducing new obligations regarding reporting back to the JPSG.[152] While the Commission proposed to enhance the EDPS' role through an authorisation on the extension of the maximum period of pre-analysis on big datasets,[153] an assessment whether personal data received from third countries is disproportionate or violating fundamental human rights,[154] and prior consultation on the launch of research and innovation projects by Europol.[155] The new regulation limits the role of EDPS. It does not need to provide prior authorisation, nor is there need for an assessment on the data provided by third countries. Only its prior consultation role for research and innovation projects has been maintained, although an exception is included. In addition, to strengthen the data protection framework, the Regulation makes several provisions of the EUDPR[156] applicable to Europol. Nevertheless, it can be questioned whether these extensions will be enough to enforce accountability by Europol if necessary. The official warning given by the EDPS in 2020 can serve as an example of how the current oversight and reporting mechanisms might not make a real difference as the disapproved practices are continued. Correspondingly, the EDPS voiced its concern about whether the legal framework regarding the oversight of Europol is sufficient for the new envisaged role of Europol.[157] The EDPS emphasises that 'harmonisation of the EDPS powers vis-à-vis Europol with the general powers of the EDPS provided in Article 58 of EUDPR' is still missing.[158] For example, the EDPS still does not have the authority to make Europol comply with the provisions of the EUDPR when it comes to processing operations, to administer consequences (such as fines) in the case of non-compliance, or to order Europol to terminate data flows to a Member State, third country or international organisation.[159] It remains unclear why this disbalance remains as possibilities are present in Article 58 of the EUDPR. The co-legislators had the opportunity to 'address

[151] Ibid., Preamble, para 16.
[152] Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final, Article 51.
[153] Ibid, Article 18(5a).
[154] Ibid, Article 18a(4).
[155] Ibid, Article 33a(1)(b).
[156] Regulation (EU) 2018/1725, Article 3 and Chapter IX.
[157] EDPS Opinion 4/2021 on the proposal for amendment of the Europol Regulation [2021].
[158] Ibid.
[159] Ibid.

the need for alignment of the EDPS powers in relation to Europol with the general powers of the EDPS'.[160] Unfortunately, the new Regulation doesn't provide this possibility even though the enhancement of power in terms of oversight by the JPSG is of particular importance considering the ability to process data that fall outside the prescribed categories during criminal investigations. The new provision has 'the most substantial impact on the protection of personal data'.[161] Therefore, in accordance with the standpoint of the EDPS, this provision should not only be applied on an 'exceptional basis', but also requires more efficient safeguards, stricter conditions and higher thresholds.[162]

5.3 Last minute changes to the Regulation

While the trialogues were ongoing, the EDPS took an additional decision. It instructed Europol to delete all the personal data not subject to Data Subject Categorisation (DSC) within a specific period of time. For data present at Europol and not subject DSC, these have to be categorised within twelve months, in the alternative they had to be deleted. For personal data received following the decision, Europol had six months to make it subject to DSC, in the alternative the data had to be deleted.[163] Although there is criticism on the EDPS its decision and the inclusion of the time limits, the Europol Regulation does prescribe it is possible to process data for the purposes in paragraph two, but limited to a period of six months. The foregoing was the start of the EDPS' reasoning, as it applied Article 18(6) 'by analogy' to the Big Data situation.[164]

Following the EDPS decision, the French Presidency proposed to introduce a new article 74a. The proposed article, upon which an agreement was reached during the trialogues, makes it possible to legalise all prior data processing. It is up to the Member State, Eurojust, EPPO, the third country or Europol itself to make sure that all data currently stored at Europol and which has not yet been subject to DSC, can still be stored legally. Interestingly, the EDPS notified Europol of its decision on the third of January 2022. The foregoing gave Europol or the legislator up until third of July 2022 to respectively comply or to alter the legislation for newly received packages.

As stated in the beginning of the paper, political agreement was reached on the first day of February 2022, with formal approval by the European Parliament and the Council on 4 respectively 24 May 2022. The text should be published in the Official Journal and enter into force before the end of June 2022, so as to avoid data deletion.

---

[160] European Parliament Legislative Observatory, '2020/0349(COD) Strengthening Europol's mandate: cooperation with private parties, processing of personal data, and support for research and innovation' (*Legislative Observatory* 1 December 2021) < Procedure File: 2020/0349(COD) | Legislative Observatory | European Parliament (europa.eu)> accessed 1 December 2021, 62.

[161] Ibid.

[162] Ibid.

[163] EDPS Decision.

[164] EDPS Decision, 4.18.

6 Regulation and Big Data

As described in the introduction, the total volume of information exchange is forecasted to grow in such an exponential fashion, that it becomes difficult to comprehend the magnitude.[165] This is acknowledged by the EDPS, as it describes how 'the number of large datasets shared by MS with Europol is rapidly growing'.[166] For Europol to enable the Member States to use new technologies and share larger datasets, the agency needs to have the necessary infrastructure available, and the capabilities to implement and adapt their internal procedures.[167] Additionally, the proposal intended to address the continuously evolving challenges Europol faces with regard to 'digital transformation, new technologies, globalisation and mobility, […] including the inter-connectivity and blurring of the boundaries between the physical and digital world'.[168] Specifically, Europol is to look at 'the development, training, testing and validation of algorithms for the development of tools'.[169] This corresponds with the wishes of Member States, as the Council of the European Union inquired prior to the Proposal: 'Europol must [make] use of artificial intelligence for analysis and operational support […] and make technologies such as artificial intelligence and encryption a priority'.[170] Consequently, the focus is also on strengthening Europol's role in the context of research and innovation projects.[171]

The new Regulation formally enables Europol to be involved in research and innovation projects; in practice, the agency has already been involved in multiple projects that focus on efficient and effective use of new technologies.[172] For example, the Europol Innovation Lab aims to find better ways to 'analyse large amounts of data to find links and new leads in investigations with machine learning tools'.[173] In addition, Europol participates in other research projects such as the Analytics for Law Enforcement Agencies (AIDA) program that focuses on creating a 'descriptive and predictive data analytics platform'

[165] Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024' (*Statistica, 7 June 2021)* <https://statista.com/statistics/871513/worldwide-data-created/> accessed 26 March 2021.
[166] EDPS Decision, 'European data Protection Supervisor's own initiative inquiry on Europol's big data challenge' [2020], para 4.6.
[167] Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final.
[168] Ibid.
[169] Ibid.
[170] Council Resolution 12463/20 on the Future of Europol [2020].
[171] Commission, 'Proposal for a regulation of the European Parliament and the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final.
[172] Europol Document 12859/20 on the EU Innovation Hub and the Innovation Lab of Europol – state of play [2020].
[173] Ibid.

which will prevent cybercrime and terrorism.[174] Moreover, the Immerse Interact Investigate (INFINITY) project aims to 'revolutionise data-driven investigations' by acting upon 'the enormous quantities of data' and to make it easier to detect cybercriminals, terrorists and hybrid threats.[175] Prior to the new Regulation, Europol had no (explicit) legal basis for these activities. The new Regulation will provide it. Once again, this illustrates how the legislation lags behind.[176] If this line of reasoning is applied to the future, this would mean that the use of newly developed tools will be repeatedly legalised after they are already being used in practice. The broad definition of the scope of the research and innovation activities in the Proposal did not contribute to breaking this cycle and ensuring necessity and proportionality.[177] Effectively, the new Regulation grants Europol a certain discretionary margin to make its own decisions regarding its future processing operations.

In addition, when it comes to addressing the rapid development in the digital environment, the new Regulation does not explicitly offer any long-term solutions or demarcations aimed to withstand the future of Big Data. The current regular practices of Member States' authorities sending Europol large and complex datasets not only creates the expectation that the agency should be capable of handling and processing these large quantities of data, but it also sets a norm: the more data, the better. Yet, as the amount of data are forecasted to grow exponentially, questions can be raised such as: What will be considered 'Big Data' in the future? The legislator seems to have anticipated the foregoing problem. The new Regulation introduces an obligation for Europol to verify whether the personal data provided is not disproportionate as regards ongoing national investigations. This explicit verification obligation for Europol entails an implied duty for the national authorities to only provide Europol personal data that is proportionate as regards their ongoing investigations. Bringing the foregoing into practice will be a true challenge. Theoretically, four options arise. Firstly, Europol violates both the verification obligation and obligation not to process data in case of manifest disproportionate data, and processes all data provided to it by the Member States. In the short or long term, the EDPS will address the violation of the verification and non-processing obligation, which excludes such option. Secondly, Europol verifies the data and, in case of disproportionality, refuses to process it. This would most certainly affect the national authorities trust in and appetite to work Europol, making this option unattractive. Thirdly, the Member States comply with their implied obligation. Given the immense staff capacity required, this option is not very realistic. Fourthly, Europol deploys its own staff, supported by new data processing procedures or AI, to the national law enforcement authorities to make

[174] CORDIS EU research results, 'Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies' (Cordis, 25 November 2021) <https://cordis.europa.eu/project/id/883596> accessed 3 December 2021.
[175] Ibid.
[176] Submission to the European Commission's consultation on revising Europol's mandate' (*Statewatch, 8 July 2020*) < eu-europol-consultation-submission-8-7-20.pdf (statewatch.org)> accessed 22 August 2021.
[177] EDPS Decision, 'European data Protection Supervisor's own initiative inquiry on Europol's big data challenge' [2020].

sure data provided to Europol is proportionate. Likely the most realistic and preferred option, it is not without complications, since it would create fixed units at national level comparable to the mobile units deployed on action days.

7 Conclusion

This paper critically analysed Europol's Big Data practices and the revision of the Europol Regulation from an EU policy perspective. It is core for Europol to analyse data in order to identify and prevent potential threats to the entire European Union. Challenges are inherent to the use of Big Data analytics yet limiting the development and use of these analytics is not a desirable alternative as Europol ought to keep up with the developments in our digital society. By making use of Big Data, Europol has been able to create insights into criminal investigations relating to cybercrime, terrorism, open-source information, and open-source intelligence. In this context, Europol mostly uses Big Data analytics to generate predictions or conduct risk analyses. In other words, when applied well, Big Data analytics offers efficient and effective operational possibilities to find the needles in the haystack when countering (serious) crime.

Europol's current mandate regulates the gathering and analysis of Big Data for the purpose of supporting the Member States in the fight against serious crime, whilst simultaneously ensuring data protection safeguards. Despite these safeguards, an official admonishment by the EDPS has addressed a breach of the data protection provisions on the processing of large datasets. In response, the Commission has proposed the revision of the 2016 Europol Regulation, which Europol explicitly supports in their Action Plan. The new Regulation contains the legal basis for Europol's extensive data processing activities by containing provisions that allow the processing of large datasets during criminal investigations.

It can therefore be stated that Europol has been operating in a way that the Council and Commission have been envisioning and that has now reflected in the new legal framework. As a result, both the current and past practice of Europol's Big Data analysing is legitimised. Since the new Regulation essentially codifies what Europol has been doing, and has been admonished for, the impact of the new Regulation will be limited in practice. Hence, the new Regulation can be described as showcasing a logic where 'the idea of what should be the case follows from an observation of what is the case'.[178] This state of affairs can be considered worrisome as there is no guarantee that Europol will not (have to) follow this line of reasoning in the future.

Moreover, while the proposal was pending, Europol did not suspend its challenged activities and thus continued its practices with minimal additional measures to regulate processing beyond its mandate. While a balance must be found between privacy and data protection on the one hand, and the protection of society against national and public

[178] Sarah Eskens, 'New and extensive data processing powers proposed for Europol', (*European Law Blog, 30 July 2021)* <New and extensive data processing powers proposed for Europol – European Law Blog> accessed 2 August 2021.

security threats on the other, the current priority of the Commission lies with the latter. Although unsurprising in the current political climate, we the taking of far-reaching measures under the umbrella of security at the cost of privacy and data protection is questionable.

It is undesirable to let Europol's wish be our command. This calls for a broad public debate on the agency's role and operation that ought to start with the delivery of bulk data by the Member States to Europol for processing. Consequently, a growing effort in data management, in general, is required. Not only must be strived for future-proof solutions that keep up with the rapidly changing world but, simultaneously, enhanced safeguards must be introduced so that fundamental rights of data subjects are ensured.

References

'Europol's European Counter Terrorism Centre strengthens the EU's response to terror' (Statewatch, 2016) <Europol's European Counter Terrorism Centre strengthens the EU's response to terror (statewatch.org)> accessed 3 April 2021.

'EU: New Europol Regulation: what the agency wants, the agency gets?' (Statewatch, 4 Augustus 2020) <www.statewatch.org/news/2020/august/eu-new-europol-regulation-what-the-agency-wants-the-agency-gets/> accessed 16 April 2021.

'Submission to the European Commission's consultation on revising Europol's mandate' (Statewatch, 8 July 2020) < eu-europol-consultation-submission-8-7-20.pdf (statewatch.org)> accessed 22 August 2021.

'Widening the net: massive expansion of Europol's data-gathering powers proposed' (Statewatch 23 February 2021) <https://www.statewatch.org/news/2021/february/widening-the-net-massive-expansion-of-eurpol-s-data-gathering-powers-proposed/, accessed 4 April 2021.

Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation [2012].

Babuta A, Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities (Royal United Services Institute for Defence and Security Studies: Occasional Papers 2017).

Babuta A and Oswald M, 'Data analytics and algorithmic bias in policing' (2019) Royal United Services Institute for Defence and Security Studies: Briefing Papers (<https://rusi.org/explore-our-research/projects/data-analytics-and-algorithms-policing> accessed 31 May 2022.

Chamon M, 'EU agencies: does the Meroni Doctrine make sense?' [2010] 17(3) Maastricht Journal of European and Comparative Law.

De Hert P and Papakonstantinou V, 'Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms' [2021] 40 Computer Law & Security Review.

Drewer D and Ellerman J, 'Europol's data protection framework as an asset in the fight against cybercrime' [2012] 13(3) ERA Forum.

Drewer D and Ellerman J, 'May the (well-balanced) force be with us! The launch of the European Counter Terrorism Centre (ECTC)' [2016] 32(2) Computer Law & Security Review.

Drewer D and Miladinova V, 'The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation' [2017] 33 (3) Computer Law & Security Review.

Emmanual I and Stanier C, 'Defining big data' in Djallel Eddine Boubiche, Hani Hamdan and Ahcène Bounceur, BDAW'16Proceedings of the International Conference on Big Data and Advanced Wireless Technologies (Association for Computing Machinery, 2016).

Ebner J, 'Exchange of views with Europol and EDPS on the implementation of Europol Action Plan to address the admonishment by EDPS following an own-initiative inquiry on internal big data challenges Exchange of views' (European Parliament, 16 June 2021) <Committee on Civil Liberties, Justice and Home Affairs - Multimedia Centre (europa.eu)> accessed 3 September 2021.

Eskens S, 'New and extensive data processing powers proposed for Europol', (European Law Blog, 30 July 2021) <New and extensive data processing powers proposed for Europol – European Law Blog> accessed 2 August 2021.

Goeman J, 'Europol under fire for use of 'targeted data' tactics in criminal investigations' NewEurope (3 February 2021) <www.neweurope.eu/article/europol-under-fire-for-use-of-targeted-data-tactics-in-criminal-investigations/> accessed 23 April 2021.

Goldsmith J, 'CJEU decides against UK government on data protection' (2020) (<www.lawgazette.co.uk/commentary-and-opinion/cjeu-decides-against-uk-government-on-data-protection/5105963.article> accessed 10 April 2021).

Kitchin R, 'Big data, new epistemologies and paradigm shifts', [2014] volume 1 issue 1 Big Data & Society, <https://journals.sagepub.com/doi/pdf/10.1177/ 2053951714528 481> accessed 19 March 2021.

Kitchin R, 'The opportunities, challenges and risks of big data for official statistics' [2015] 31(3) Statistical Journal of the IAOS.

Köning F, 'Big Data, 5G and AI: How Europol could help Von der Leyen achieve her goals' (Hertie School: Jacques Delors Centre 2020)

Lomas N, 'Europe's top court confirms no mass surveillance without legal limits' (2020) <https://techcrunch.com/2020/10/06/europes-top-court-confirms-no-mass-surveillance-without-legal-limits/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMoBTOl8eVwYj4kQbNcPWrBez8b5xfdtofb9LvMdfU8m3djvSK6RHwY4Il551_PNrPfabof5Nqjf4RW2lrDPJ5ol79B-9DtEz6EWsIoilng5iLqnaEwd1JMLqxOmitKWfZxjP6M3Dg2u0Tyd2Mftq9LnuFRCXf9ZXNM8fuE3_29E> accessed 31 May 2022.

Manancourt V and Wanat Z, 'EU regular warns Europol could be breaking data rules', Politico (20 October 2020) <www.politico.eu/article/eu-regulator-warns-europol-could-be-breaking-data-rules/> accessed 26 March 2021.

Monroy M, 'Europol uses Palantir' (2020) (<https://digit.site36.net/2020/06/11/europol-uses-palantir/> accessed 26 March 2021).

Oberwittler D and Roché S, Police citizen relations around the world. Comparing sources and contexts of trust and legitimacy (1st ed, Routledge, 2019).

Van der Wagen W, Oerlemans J and Weulen Kranenberg M, (eds), Basisboek cybercrime. Een criminologisch overzicht voor studie en praktijk, 1st ed, Boom Lemma 2020, 49.

van Erp J, Stol W and van Wilsem J, 'Criminaliteit en criminologie in een gedigitaliseerde wereld' [2013] 55 (4) Tijdschrift voor Criminologie.

Vavoula N and Mitsilegas V, 'Strengthening Europol's mandate A legal assessment of the Commission's proposal to amend the Europol Regulation' (2021) European Parliament Policy Department for Citizens' Rights and Constitutional Affairs <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694200/IPOL_STU(2021)694200_EN.pdf> accessed 3 September 2021.

Zalnieriute M, 'The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments' [2020] 24(28) American Society of International law.

Until the end of the 1990s, EU integration in the area of criminal law centred primarily around the regional deepening of traditional judicial cooperation in criminal matters and the development of law enforcement cooperation (including the setting up of Europol as a support agency). By the end of the 1990s respectively 2000s, the EU also gained (limited) supranational competence in the areas of substantive respectively procedural criminal law. Both judicial and law enforcement cooperation were furthered over the years via the principles of mutual recognition respectively availability, and through the setting up (and development) of Eurojust, the establishment of a European Public Prosecutor's Office and the further development of Europol. After three decennia, the EU criminal law corpus is impressive – a core component of the EU's 'Area of Freedom, Security and Justice', building on and adding to (both real and presumed) trust between the Member States.

No time for stand-still, though. Since 2020, the European Commission has launched a tsunami of new legislative proposals, including in the sphere of EU criminal law, strongly framed in its new EU Security Union Strategy.

This special issue on 'EU criminal policy. Advances and challenges' discusses and assesses some of the newest developments, both in an overarching fashion and in focused papers, relating to key 2022 novelties for Europol (ie the competence to conduct AI-based pre-analysis in (big) data sets, and extended cooperation with private parties), the sensitive debate since 2020 on criminalising (LGBTIQ) hate speech and hate crime at EU level, the 2022 Cybersecurity Directive, the potential of the 2020 Conditionality Regulation to address rule of law issues undermining the trustworthiness of Member States when issuing European Arrest Warrants, and concerns about free speech limitation by the 2021 Terrorist Content Online Regulation.

Gert Vermeulen is Senior Full Professor of European and international Criminal Law and Data Protection Law, Director of the Institute for International Research on Criminal Policy (IRCP), of the Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES) and of the Smart Solutions for Secure Societies (i4S) business development center, all at Ghent University, Belgium. He is also General Director Publications of the AIDP and Editor-in-Chief of the RIDP.

Wannes Bellaert is PhD Researcher and Academic Assistant at the Institute for International Research on Criminal Policy (IRCP), Ghent University.

www.maklu.be
ISBN 978-90-466-1134-0