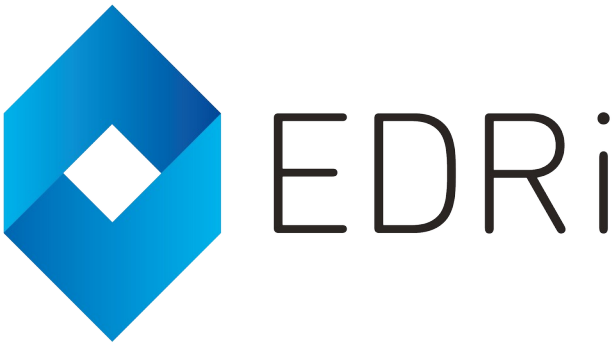

Recommendations on the revision of Europol's mandate

Position paper on the European Commission's proposal 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

10 June 2021

Table of Contents

Executive summary

European Digital Rights (EDRi) is the voice of 45 organisations and gathers NGOs, experts, advocates and academics working to defend and advance human rights in the digital era in Europe and beyond. This paper was developed with the contribution of our members IT-Pol Denmark, Statewatch.

EDRi recognises the importance of adequate measures to fight serious crime but is concerned that the reform of Europol's mandate is taking a wrong direction. If adopted, the European Commission's new proposal for a Regulation 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 would have tremendously negative effects on the fundamental rights of affected persons, both suspects and innocents.

In this Position Paper, EDRi criticises the expansion of competences attributed to Europol without due consideration of its legal mandate as defined by the treaties and a proper evaluation of the efficiency and human rights compliance of its current missions and practices. That's notably the case where the Commission proposes to ease data transfers with third countries, although no evaluation was carried out on the circumstances under which Europol and national law enforcement authorities derogate from the current rules. Likewise, contrary to what the Commission proposes, Europol should not be allowed to enter alerts in the Schengen Information System, because it runs counter to the treaty provisions governing the Agency and raises significant legal and human rights concerns which were not properly evaluated.

According to the Commission proposal, Europol would also be able to directly request personal data from private companies in order to identify which Member States are responsible for launching an investigation and transmit to them evidence received from private entities. This system promotes the voluntary disclosure of personal data by online service providers (that should normally be obtained via legal means), which goes against the EU Charter of Fundamental Rights, the principle of the rule of law and national and European procedural safeguards. The Agency would also transfer data to feed into platforms' automated content filtering tools in order to "address the dissemination of online terrorist content", thus reinforcing Europol's censorship powers, incentivising the use of error-prone technologies with a high risk of legitimate content being deleted and creating chilling effects on freedom of expression online.

Furthermore, we deplore the blank cheque given to Europol to circumvent its own rules by allowing the analysis of data categories it should ordinarily not process at all for the purpose of supporting Member States' criminal investigations. Instead of creating easy-to-abuse loopoles in Europol's legal framework, the EU would do well to launch a democratic debate on the rise of hacking techniques, data mining and mass surveillance in law enforcement in Europe and to question their impacts on people's fundamental rights and trust towards public institutions.

Lastly, the proposal suggests that Europol should play a bigger role in developing and shaping future policing technologies that will be deployed in Europe in the coming years. For that, the Agency would help set the pri-

orities in terms of EU funding for research projects in the field of security and train and test itself algorithms to develop tools for EU law enforcement authorities. Given the impacts of these assistive technologies on the lives and rights of persons and communities subject to them, we argue that such role should not be given to an opaque and unaccountable agency. Instead, we believe the involvement of democratically elected bodies and of representatives of affected groups – mainly marginalised communities - should be actively sought and guaranteed when making decisions over the future of policing tools, practices and strategies.

Introduction

On 9 December 2020, the European Commission released its proposal to amend the Europol Regulation that constitutes the legal framework defining the activities of the European agency for law enforcement cooperation. This revision comes only 3 years after the entry into force of the current regulation and 2 years before the deadline of the first implementation evaluation report (set for 2022).

In its response to the Commission's consultation on the inception impact assessment, EDRi outlined its concerns about the appetite to speed up the reform of the agency's mandate without a proper assessment demonstrating that the current practices are unfit for purpose.[1] Without this evaluation, it is impossible to assess whether the current rules impede the fulfilment of the agency's mission. This type of assessment is of utmost importance in light of the legislative initiative's broad objectives to extend Europol's operational powers in terms of data processing and to overcome "restrictions in the Europol Regulation".[2]

The Commission's proposal seeks to achieve the following objectives:

1) Objective I: Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals.

2) Objective II: Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights.

3) Objective III: Enabling Member States to use new technologies for law enforcement.

The stated overall objective is therefore to expand Europol's capacities to access personal data, to process it on a mass scale for analytics and to promote the development and use of technologies and methods which employ artificial intelligence (AI), machine learning, big data and augmented reality for law enforcement. This expansion comes at a time when the European Data Protection Supervisor (EDPS), the entity responsible for monitoring and ensuring the application of fundamental rights and freedoms protections by Europol, has deeply criticised Europol.[3] Following an investigation in 2020, the EDPS raised three serious concerns: (1) Europol receives huge amounts of data on individuals from Member States, among which there are categories of personal data that go beyond the necessarily limited list permitted by the Europol Regulation, including data pertaining to individuals who are in no way connected to criminal activities; (2) Europol uses such data to test and develop algorithms for law enforcement activities without a clear legal basis; and (3) Europol allows national investigators to help with the data analysis, again without legal basis.[4] The discrepancy between Europol's current practices and its legal framework reinforces the impression that the presented changes to Europol's mandate are an attempt to legalise the agency's unlawful activities.

---

1 EDRi, *Feedback to the Roadmap to revise the mandate of the European Agency for Law Enforcement Cooperation (EUROPOL)*, 8 July 2020, available at: https://edri.org/wp-content/uploads/2020/07/EDRiResponseEuropolRegulation.pdf

2 European Commission, *Impact Assessment Report*, SWD(2020) 543 final, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate

3 European Data Protection Supervisor, 'Invitation to the Seventh JPSG meeting on 28-29 September 2020', available at: https://www.europarl.europa.eu/cmsdata/211695/EDPS_letter_23092020.pdf

4 Idem

Furthermore, Europol's work cannot be considered in isolation from the wider political context.[5] 2020 was a year of heightened public awareness and contestation of police abuses, and the reconsideration of the role of the police more generally in the EU. Across the continent, there is plenty of evidence to demonstrate the role of police in perpetuating structural racism, in particular through practices of racial and ethnic profiling (although forbidden by the European Convention on Human Rights and the EU Charter of Fundamental Rights), racially-motivated police violence and crimes – such as abusive stops and searches, surveillance measures and arrests, targeting in particular racialised people and migrants. Europol heavily relies on the activities and actions of national law enforcement authorities and thus the data it receives from them to carry out data analysis reflects these discriminatory practices. Consequently, it sustains the trends of criminalisation and overpolicing of already marginalised communities at European and national levels. These concerns highlight the important gap of understanding regarding how and to what extent Europol's analytical work is influenced by national law enforcement activity and in turn, how this work skews national operations.[6] It is regrettable that neither the Council of the EU[7] nor the European Commission[8] has addressed this issue as part of the revision of the Europol Regulation (instead of considering it as a mere negative impact to mitigate).

The European Parliament's (EP) Civil Liberties, Justice and Home Affairs Committee (LIBE) and the Council of Member States expected to amend and vote on the proposed revision of Europol's mandate as well as of the Regulation establishing the Schengen Information System in 2021. EDRi proposes the following recommendations regarding the provisions related to the protection of human rights in the digital environment.

EDRi supports the aim of achieving a coherent and effective response to serious crime and terrorism. However, EDRi has deep concerns relating to numerous provisions, in particular insofar as they present premature revisions without regard to due process and create numerous dangerous legal shortcuts. The revised Europol regulation will lower several of the safeguards included in the 2016 Regulation and set up new operational duties that are both opaque and not subject to parliamentary scrutiny or judicial oversight. This policy agenda does not uphold the necessary transparency requirements to ensure that Europol remains a fully democratically accountable organisation. EDRi therefore encourages the EU legislators to consider the following recommendations.

5 Statewatch, 'Europol: plans afoot to legalise unlawful acts', 9 July 2020, available at: https://www.statewatch.org/news/2020/july/europol-plans-afoot-to-legalise-unlawful-acts/#_ftnref3

6 Statewatch, 'Big data experiments: new powers for Europol risk reinforcing police bias', 11 February 2021, available at: https://www.statewatch.org/news/2021/february/big-data-experiments-new-powers-for-europol-risk-reinforcing-police-bias/

7 Justice and Home Affairs Council, 'Outcome of the Council meeting', 2-3 December 2019, available at: https://www.consilium.europa.eu/media/41586/st14755-en19.pdf

8 European Commission, *Impact Assessment Report,* SWD(2020) 543 final, part 1/2

The reform of the Europol Regulation should be based on evidence

- EDRi recommends the European Commission to first carry out a full and public evaluation of the 2016 Europol Regulation before reforming the Agency's mandate.

In its Roadmap, the European Commission states that it does not intend to carry out an evaluation of Europol's current mandate because "the amount of evidence that can be collected for the purpose of a fully fledged evaluation is limited and non representative".

The Commission commissioned a study on the on the practice of direct exchanges of personal data between Europol and private parties in order to identify the shortcomings in the current system under Article 26(2), under which Europol is only allowed to process personal data with the sole purpose of identifying the jurisdiction concerned.[9] However, a briefing published by the European Parliament's Research Service stresses that the study "suffers from a number of shortcomings. It does not address (the need for) independent judicial control, nor does it properly reflect the positions of national data protection authorities (DPAs) and private parties."[10]

It is highly surprising that the EU Commission proposes a revision of Europol's rules before even the first implementation and review cycle of five years (Article 68) is complete. The first fully fledged evaluation of the Regulation is planned for 2022 to assess the effectiveness and efficiency of Europol and of its working practices. However, the Commission and the Council[11] already foresee the revision of the mandate, before there is any evidence that the current practices are unfit for purpose. **EDRi recommends to first carry out a full and public evaluation of the 2016 Europol Regulation before reforming the Agency's mandate.**

Allowing extralegal data exchanges between Europol and private parties

- EDRi opposes the extension of Europol's mandate to transfer and request personal data from private parties as: (1) it promotes the voluntary disclosure of personal data by online service providers, which goes against the EU Charter of Fundamental Rights, the principle of the rule of law and national and European procedural safeguards; (2) it goes beyond Europol's legal basis (Article 88(2)).
- Amendments to existing Article 26 should be rejected.
- Article 26a on "Exchanges of personal data with private parties in crisis situations" should be deleted. If pursued, the definition of "crisis situations" should at least be strictly limited to the prevention of the dissemination of online content related to terrorism in situations where such content incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541 directly threatening the life or physical integrity of a person.

9 Milieu, *Study on the practice of direct exchanges of personal data between Europol and private parties*, September 2020, available at: https://ec.europa.eu/home-affairs/sites/default/files/e-library/docs/pdf/publication_study_private_parties.pdf

10 European Parliamentary Research Service, 'Revision of the Europol Regulation', Briefing, PE 654.214, January 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/654214/EPRS_BRI(2021)654214_EN.pdf

11 https://data.consilium.europa.eu/doc/document/ST-14745-2019-INIT/en/pdf

> *"It should also be noted that the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter [of Fundamental Rights of the European Union], and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter." - Court of Justice of the European Union, Case C-623/17.*[12]

The first objective of the reform is to enable Europol to receive and request personal data from private parties. Private parties include online platforms and telecom companies, banks and financial institutions, but also illegal online content reporting centers (also called "internet hotlines"),[13] etc. For Europol and the European Commission, the problem lies with the fact that private parties hold lots "of non-attributable or multi-jurisdictional data sets relevant for law enforcement authorities in multiple jurisdictions". The aim of the proposal is to allow Europol to receive this data and to analyse it in order to determine which Member States would be in charge of launching criminal investigations. With the reform, the private parties will therefore be encouraged to voluntarily disclose data to Europol that could be of interest because it might pertain to serious crimes or ongoing criminal investigations in several European countries (also called "criminal intelligence"). The personal data would be processed by Europol in line with its existing legal framework. The Agency would – in a first step – process the data in order to determine whether such data are relevant to its tasks (they relate to serious crimes falling in Europol's mandate such as the fight against terrorism or organised crime). In a second step, and if the data is relevant to its tasks, the Agency would analyse it to identify the relevant jurisdictions and share it with the Member States concerned.

Lastly, the European Commission also wants Europol to serve as a channel to transmit requests from Member States containing personal data to private parties. It argues that national law enforcement authorities could benefit from using Europol's infrastructure when exchanging critical information amongst each other or with private parties in the context of large scale cyber attacks.

As the cooperation between private parties and Europol includes the processing of personal data, the assessment of policy options to achieve the identified objective needs to take full account of fundamental rights and notably the right to the protection of personal data, the right to privacy and freedom of expression.

12 CJEU, Privacy International, C-623/17: http://curia.europa.eu/juris/document/document.jsf;jsessionid=CFAA160AC259FF995ABBB73585790AD5?text=&docid=232083&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8422287

13 The impact assessment takes as example the US National Center for Missing and Exploited Children (NCMEC), a reporting center, which cannot transmit to Europol the information it holds on the sharing of child sexual abuse material online and therefore has troubles identifying which jurisdictions are concerned (page 21).

1. Europol must not serve to circumvent procedural safeguards and accountability mechanisms by sharing and requesting follow-up data directly to private companies

> *"The Agency was set up to provide services which help Member States overcome the limitations of their national 'toolboxes', in particular by helping them to access relevant personal data held by other Member States" - European Commission's impact assessment, 2020*

As per its mission, Europol's main task is to "collect, store, process, analyse and exchange information" that it gathers from Member States, EU bodies and "from publicly available sources, including the internet and public data". Europol was deliberately founded without executive powers. It is only supposed to notify Member States of possible criminal offences in their jurisdiction, not start investigations on its own. Thus, after notification, it is for the respective Member State to decide whether to investigate or not. If a Member State decides to take action, Europol can provide support, including by participating in joint investigation teams. However, Member States increasingly advocate to expand Europol's "operational" capacities and its power of initiative, which (1) is not matched with a stronger system of checks and balances and (2) is at odds with Europol's legal basis.

The main example of the growth of Europol's operational mission is the creation of the Europol Internet Referral Unit (IRU), which is tasked to monitor the internet and look for content that is likely to be "incompatible" with the terms of service of online service providers like Facebook, so that the latter can "voluntarily consider" whether to delete it or not. The IRU does not possess the competence to assess the legality of online content itself (e.g. to interpret legal provisions determining the limits to freedom of speech, and to distinguish illegal from harmful yet legal content).[14] Yet it can put pressure on companies to delete content without any responsibility or accountability for potential over-removal of legal content. This mechanism certainly does not comply with the EU Charter's requirement that restrictions (on freedom of expression in this case) of fundamental rights must be "provided for by law", not based on opaque "cooperation" between law enforcement authorities and private companies.

Article 26a of the proposal expands Europol's *de facto* operational powers for terrorist content online by allowing Europol to request and receive personal data directly from private parties to prevent the dissimination of online content or violent extremism in crisis situations. The definition of "crisis situations" in Article 4(1)(u) focuses heavily on the potential for exponential multiplication and virality of content across multiple online service providers, which may cover a large number of cases where allegedly violent extremist content is posted by random users on social media plaforms. With such a broad definition of "crisis", the operational powers will be exercised on a systematic scale rather than on an exceptional basis. The broad mandate for Europol to exchange personal data with private parties in order to prevent the distribution of allegedly extremist content (through referrals) can have a chilling effect on freedom of expression and the right to information. Recital 35 foresees that Europol exchange hashes (fingerprints) of extremist content with private parties for the pur-

14 EDRi, 'All Cops Are Blind? Context in terrorist content online', 13 February 2019, available at: https://edri.org/our-work/context-in-terrorist-content-online/

pose of blocking such content across different platforms.[15] Hashes are effective in recognising known content (especially images), but remain ineffective in accurately assessing the context of the publication. Content disseminated for journalistic, educational and artistic purposes or for raising awareness of the horrors of terrorism (such as counterspeech) is likely to be blocked by automatic upload filters.[16]

Likewise, the existing Article 26 is amended in a way that gives Europol new powers of initative and to carry out genuine law enforcement activities on its own. Europol would be allowed to "receive and, in specific circumstances, exchange personal data with private parties". According to the draft Regulation, service providers would like to share "lawfully and voluntarily" data that they hold about their customers and that would be relevant for several law enforcement authorities. However, they are often unable to identify which jurisdiction is responsible. The reform suggests that Europol takes up that task by receiving data sets voluntarily shared by service providers and analysing them in order to identify which national jurisdictions are concerned and to transfer them that data. In cases where the information provided is insufficient to identify which Member States are concerned, the Agency would be authorised to request further information from the service provider. In these situations, the private companies are expected to decide by themselves whether or not they want and are allowed under the law to share additional information with Europol, and if so, which information. Furthermore, if the service provider does not follow up Europol's original request, Europol can submit a request under Article 26(6a) to the Member State in whose territory the service provider is established to obtain additional personal data.

This proposal is problematic on many levels. Since Europol is not a competent authority with executive powers, the proposal for direct cooperation with private parties would institutionalise a system of voluntary disclosure of personal data by online service providers and other private companies without providing any legal basis for the processing of personal data (disclosure) by data controllers.

EDRi has consistently opposed voluntary disclosures of personal data since this represents further processing of that data by the private controller for a purpose inconsistent with the original purpose. Disclosure of personal data to law enforcement bodies should always be regarded as a restriction of fundamental rights that must be provided for by law and satisfy requirements of necessity and proportionality in accordance with Article 52(1) of the Charter of Fundamental Rights. There is an inherent logical contradiction between disclosures that would be both "voluntary" for private companies and "necessary" for objectives of general interest. The voluntary disclosure takes place without the procedural safeguards that apply to Member States' law en-

15 The main hash database of known terrorist content online is currently overseen by the Global Internet Forum To Counter Terrorism. It was developed initially by Facebook, YouTube, Microsoft, and Twitter as a voluntary measure in 2016. It contains digital hash "fingerprints" of images and videos that platforms have identified as "extreme" terrorist material, based not on the law but on their own Community Guidelines or Terms of Service. The platforms can use automated filtering tools to identify and remove duplicates of the hashed images or videos. As of 2018, the Database was said to contain hashes representing over 80,000 images or videos. This filtering tool seriously threatens people's rights to seek and impart information as the definition of "terrorist content" is unclear and not based on the law. See EDRi, 'Open letter on the Terrorism Database', available at: https://edri.org/our-work/open-letter-on-the-terrorism-database/

16 This critique was raised against the (voluntary) upload filters in the Terrorist Content Online Regulation. Europol's operational powers in Article 26a are likely to exacerbate the problems with upload filters for freedom of expression by putting increased pressure on private platforms to block content through the direct exchange of hashes and other personal data with private parties.

forcement authorities when seeking access to personal data in accordance with national or Union law, e.g. prior review by a court or an independent administrative body. This may incentivise a structural shift in data collection practices from Member States' authorities to Europol in order to avoid what may be perceived as "red tape" obstacles, which would have a detrimental effect on fundamental rights. The Commission's impact assessment mentions a "reduction of the administrative burden for national law enforcement authorities" as a likely impact of Europol "cooperating in a direct and more efficient way with private entities", without considering the potential adverse implications for fundamental rights.

Furthermore, the possibility for Europol to directly receive information by private parties is limited by its own legal basis. Article 88(2) states that Europol's tasks may include the "collection, storage, processing, analysis and exchange of information, in particular that *forwarded by the authorities of the Member States or third countries or bodies.*" (emphasis added). Receiving and actively requesting data from private companies on a large scale extends far beyond this legal basis, exponentially expanding the operational reach of Europol without due justification.

Lastly, the additional power of directly requesting private companies for additional data would be granted outside of the long-standing judicial cooperation framework and would certainly fall short of the rights-protective procedural requirements as well as of strong judicial oversight required under the rule of law.

The proposal also provides for a mandatory disclosure regime which effectively gives Europol operational powers. Member States are required to ensure in their national law that their competent national authorities can receive and process requests from Europol for personal data held by private parties.[17] In effect, Europol is granted similar operational powers as an issuing authority under the European Investigation Order (EIO) Directive with Member States as the executing authority. The proposal does not lay down clear and precise rules governing the scope and application of the new requesting powers for Europol, as is required for any interference with fundamental rights in EU law. The Commission's impact assessment confounds the lack of clarity by stating that requests from Europol should not "go beyond what national law enforcement authorities of said Member State could request without judicial authoritisation",[18] which, depending on the implementation by Member States, could either make the scope of the provision rather limited (very little information can be obtained without a court order) or contradict the jurisprudence of the CJEU that holds in a number of cases that authorisation from a court or independent administrative authority is needed to compel private parties to disclose personal data to law enforcement authorities.

2. Access to personal data should respect the principle of territoriality and should only be granted with prior judicial authorisation

The current rules are intended to prevent Europol from breaching procedural rules governing the collection and processing of evidence in Member States. Direct "cooperation" with service providers, whereby Europol or police officers in another Member State directly request data from the providers, affects the territorial sovereignty of Member States in which the order is executed (executing State). As a result, the executing State

17 Article 1, point 12 - point d [Article 26, paragraph 6a] and recital (31) in the proposal
18 European Commission, *Impact Assessment Report,* SWD(2020) 543 final, part 1/2, page 47

cannot effectively fulfil its responsibility to protect the fundamental rights of individuals affected since it has no knowledge of the data transfers taking place. Procedural rules for the collection and processing of personal data in criminal matters guarantee that collected evidence will not be declared inadmissible by the courts later. It is especially important when seeking a suspect's identity through the collection of metadata (e.g. IP addresses) that this identification relies on evidence acquired in the respect of procedural rules. Otherwise, the rest of the investigation would be at risk.

In order to ensure legal certainty for national investigating officers and to respect the principle of territoriality, Europol should not be allowed to request and process personal data without the authorisation of the executing authority as foreseen in Article 26(5). EDRi believes that access to personal data by Europol must be validated by the competent authority in the executing State in order to ensure the verification of immunities or other specific protections granted by national laws that restrict the access to certain categories of personal data or even the respect of their national security interests.

Under the current proposal, the missing information requested by Europol to identify national units concerned (1) must have a clear link with the information previously shared by the private party (para. (d)(ii)) and (2) is strictly limited to what is necessary for Europol to identify the national units concerned (para. (d)(iii)). Recital 30 further indicates that it is up to the private parties to "*decide* whether it is in their interest to share additional information with Europol and *whether they can lawfully do so*". As part of the rule of law, a private party should not be asked to either assess the legality of a data transfer or determine which information meets the necessity criteria set in paragraph (d)(iii). Expecting the opposite would put companies at the same level as a court or a state, which is simply unacceptable in the EU legal order. States have legal and democratic obligations to respect and defend people's fundamental rights. Companies do not have such obligations. If companies are left to decide whether or not handing over citizens' data, people's rights are put at risk. For example, as noted by the Council of Bars and Law Societies of Europe and the German Bar Association [19], service providers are in no position to guarantee that the lawyer-client privilege is respected. Moreover, it certainly does not bring legal certainty for all parties involved (the affected persons and the private parties).

The same conclusion applies to Europol. Judicial review and validation by a competent authority are, always required when fundamental rights interferences are at stake. As established by the Court of Justice of the European Union (CJEU), this judicial oversight helps to verify that the collection of data can bring an effective contribution to the prosecution of a specific crime. The judicial authority is required to make sure that the data request meets the necessity and proportionality tests. Furthermore, judicial review and validation should only be carried out by a court or an independent administrative authority in accordance with CJEU jurispru-

19 CCBE, *Position Paper on the Proposal for Regulation 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*, 6 May 2021, available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20210506_CCBE-position-paper-on-Europol-s-mandate.pdf
Deutscher Anwaltverein, *Position Paper of the German Bar Association by the Committee on Criminal Law on the Proposal for a Regulation COM(2020) 796 final 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*, 15 April 2021, available at : https://anwaltverein.de/de/newsroom/sn-31-21-zum-vorschlag-f%C3%BCr-eine-verordnung-com2020-796-final

dence. Considering the functions granted to Europol by the Treaties, the Agency cannot possibly meet the criteria of a competent authority under EU law and cannot determine if an interference with fundamental rights as a result of a data request is necessary and proportionate. **Therefore, Europol should only be allowed to receive personal data held by private companies if competent authorities in the Member State of establishment have obtained it under its applicable national law in accordance with Union law and submitted it to Europol.**

Enabling Big Data analysis to feed a data-driven policing model

- Europol should strictly abide by the list of data categories established in Annex II of Regulation (EU) 2016/794 in all circumstances and therefore, Article 18a should be deleted.
- Responsibility for verifying the legality of data transfers to Europol should remain with the Member States and countries and organisations with which Europol has operational agreements. When Member States' authorities submit personal data to Europol for cross-checking or operational analysis, they should ensure that the datasets only contain information that Europol is allowed to process, indicate the categories of data subjects under which the data falls and, in any case, refrain from knowingly sending information that Europol is not allowed to process.
- If, following a processing, Europol discovers that it is not allowed to process certain parts of a dataset received by a Member State or a third party, it should stop the processing, inform the submitting entity and promptly delete the dataset received.
- The European Parliament should follow-up on its two resolutions[20] on electronic mass surveillance of EU citizens, evaluate the state of implementation of its recommendations and whether they demand additional actions in order to prohibit blanket mass surveillance activities and bulk processing of people's personal data.
- The European Parliament should commission a comparative study on the existing law enforcement and police scrutiny bodies and/or mechanisms at national level (responsible for receiving and handling complaints as well as to perform audits of law enforcement authorities' compliance with fundamental rights legal requirements) in order to inform the reform of Europol's scrutiny mechanisms. The study should aim at identifying best practices and innovative measures in terms of standards of independence, composition, transparency and accountability mechanisms, role and tasks, taking into account the extent to which scrutiny bodies at national level facilitate meaningful participation by marginalised communities.
- The work of the JPSG should be evaluated in order to determine whether or not it has been able to carry out its missions before the new mandate is adopted and if not, amended as follows:
- The JPSG should be given real powers of supervision by: (1) enabling its scrutiny of Europol's day-to-day work and the issuance of binding recommendations; (2) granting it decision powers in the appointment of the Executive Director and Deputy Directors;
- The possibility of granting the JPSG voting rights in Europol's Management Board should be evalu-

20 European Parliament, *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, P7_TA(2014)0230, available at: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.pdf
European Parliament, *Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens*, P8_TA(2015)0388, available at: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0388_EN.pdf

ated.

1. The identification of Europol's unlawful practices should not lead to the creation of loopholes in Europol's legal basis

In April 2019, Europol informed the EDPS of "serious compliance issues" concerning its data practices and invited the EU data protection authority to look deeper into the matter.[21] A year later, the EDPS released the results of its investigation, warning that Europol was currently processing personal data that mainly refers to individuals not linked in any capacity to any criminal activity and therefore, data categories that go way beyond what Europol is allowed to process and store.[22] The fact that the Agency itself had to raise the issue highlights the severe concerns we have as regard the capacity of its watchdogs – the EDPS and the Joint Parliamentary Scrutiny Group (JPSG) - to effectively oversee its day-to-day work.

These findings inspired the European Commission to address this "structural legal problem"[23], encouraged by EU Member States[24] who called for "any possible action [to] be taken to minimise the impact of the EDPS decision".[25] As a result, the Commission proposes new provisions that would simply allow Europol to "exceptionally" circumvent its rules on data processing. Instead of suggesting solutions to bring Europol's practices in line with its mandate, the Commission proposes to adapt the current legal framework to align with Europol's data processing activities. The aim is therefore to adjust the legal basis to the current unlawful reality, which raises serious concerns with regards to the respect of the EU's 'better regulation' principles and the state of the European democratic deficit.

> *"(...) the policy option would **safeguard the status quo** of Europol's work in supporting Member States by way of data processing" - European Commission's impact assessment, 2020, emphasis added*

What the Commission proposes is to allow Europol to analyse large datasets, received from national law enforcement authorities and likely containing personal data that Europol is normally not allowed to process, in two cases: (1) to check whether the data received falls within the remits of the data categories that Europol is allowed to process[26] (i.e. data related to suspects, convicted persons and persons who are suspected to commit a crime in the future, contacts and associates, victims, witnesses and informants). The Commission calls it a "pre-analysis" because it is supposed to take place before the data is processed for operational purposes; and (2) When Europol is faced with a "large and complex data set", it can "exceptionally" analyse and store it,

21 S. Stolton, 'Europol on defensive as concerns raised over 'illegal' Big Data tactics', 2 February 2021, available at: https://www.euractiv.com/section/digital/news/europol-on-defensive-as-concerns-raised-over-illegal-big-data-tactics/

22 European Data Protection Supervisor, 'Invitation to the Seventh JPSG meeting on 28-29 September 2020', available at: https://www.europarl.europa.eu/cmsdata/211695/EDPS_letter_23092020.pdf

23 European Commission, *Impact Assessment,* SWD(2020) 543 final, 9 December 2020, page 23.

24 In the framework of the Law Enforcement Working Party (LEWP) which is a Council preparatory body, which handles work relating to legislative activities as well as cross-border policing and related operational issues. This includes activities related to Europol.

25 European Commission, *Impact Assessment Report,* SWD(2020) 543 final part2/2, page 16

26 Annex II, 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

even if it contains the data of non-suspects. This "exception" from the existing rules would be regulated with several purported safeguards (such as a clear definition of the situations where the exception can be applied, notably in cases where the processing is supporting a specific criminal investigation in a Member State).

1.1 Pre-analysis of large data sets encourages "NSA-style" data mining of indiscriminately collected data sets

The proposed paragraph 5a of Article 18 allows Europol to "temporarily process" personal data for the purpose of determining whether such data complies with the requirements of Article 5, in particular the specific categories of personal data and categories of data subjects in Annex II. Viewed in isolation, this pre-analysis can contribute to ensuring that Europol's subsequent information processing activities stay within the remit of the Europol Regulation as personal data falling outside the remit (Annex II) must be deleted, although not immediately.[27]

In a broader context, the pre-analysis provision encourages general and indiscriminate collection of personal data and the subsequent use of data-mining[28] analysis to identify unknown "persons of interest" whose personal data can then be lawfully processed for combating crime by Europol and Member States' competent authorities. This data mining, which resembles the *modus operandi* of intelligence services such as the U.S. National Security Agency (NSA), can circumvent critical safeguards in criminal procedure law and the presumption of innocence.

The proposal contains no safeguards or limitations regarding the collected large datasets which can be subjected to pre-analysis. This can lead to inferences with the right to data protection and other fundamental rights that are not properly circumscribed by law as required by Article 52(1) of the Charter of Fundamental Rights. The risk of unlawful interferences with fundamental rights is particularly pertinent when considering that the whole premise of pre-analysis is that some of the collected data cannot be processed lawfully by Europol. Under the case law of the CJEU, legislation permitting the collection of personal data must meet objective criteria that establish a connection between the data to be collected and the objective pursued. Interferences with the right to privacy and data protection must be limited to what is strictly necessary, a requirement which also applies to the initial data collection. It is not sufficient for the legislation to provide safeguards for the subsequent access to that data or use pre-analysis to determine whether the data should be retained or deleted.

The Commission uses the recent joint investigation to dismantle EncroChat to justify the need for Europol to process large datasets.[29] Through this investigation, law enforcement authorities in France and the Netherlands obtained access to electronic communications data for a large number of individuals suspected of various crimes. According to the Commission, since the EncroChat network had users throughout the European Union, analysis of the obtained data by Europol was instrumental in distributing information to other Member

27 Europol can retain the full data for a year, or in justified cases for a longer period, while carrying out the pre-analysis.
28 Data mining is a process of extracting and discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems.
29 EncroChat was an encrypted phone network used by some criminal networks. See J. Cox, 'How Police Secretly Took Over a Global Phone Network for Organized Crime', *VICE*, 2 July 2020, available at: https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked

States.

While the EncroChat case is presented as a success story for pan-European law enforcement, it also highlights a number of problems with the proposed processing of large datasets by Europol. Communications data from the EncroChat network was obtained in a general and indiscriminate manner where all users were subjected to bulk hacking (sometimes referred to as "bulk equipment interference"). Instead of an individualised suspicion to justify the extremely intrusive measure of government hacking and interception of private communications, the French and Dutch authorities simply assumed that most EncroChat users were criminals.[30] Clearly, the French and Dutch authorities could not reasonably have known this beforehand due to the highly anonymous nature of the EncroChat network (which in itself is not illegal). In the aftermath of the EncroChat investigation, it has been revealed that law enforcement authorities gained access to potentially privileged communications between lawyers and their clients, which is is breach of the law granting special protection to data exchanged and communications between lawyers and their clients[31] or between journalists and their sources. The EncroChat userbase is also likely to have included journalists, whistleblowers and human rights defenders[32], all of whom have legitimate needs for strong privacy protection.

Bulk hacking operations like the EncroChat investigation are not necessarily legal in every Member State. Even in Member States that have provisions for bulk hacking, the legality of an investigation like EncroChat can be highly uncertain.[33] Furthermore, since the users of EncroChat and their geographical location were largely unknown before initiating the bulk hacking operation, the French and Dutch authorities effectively conducted their investigation on the territories of other Member States without any regard to the domestic rules and safeguards for interception of private communications. When Europol analyses and "distributes" communications data obtained in bulk in this manner, at least some Member States' authorities may have received information which they could never have obtained legally in a domestic investigation. This raises a number of issues related to the right to a fair trial, especially as the origin of the information received via Europol may not be fully revealed in the domestic investigation.[34]

30 The French authorities claimed that they estimated that no less than 90% of *EncroChat* clients were linked to organised crime. If these numbers are true, it means that potentially up to 6000 users had their fundamental right to privacy infringed. See *France24*, European police shut criminal phone network used to plan murders, 2 July 2020, available at: https://www.france24.com/en/20200702-european-police-shut-criminal-phone-network-used-to-plan-murders

31 See footnote 19

32 Investigative journalist Rebecca Tidy mentions in her piece that she occasionally used Encrochat to speak to contacts wishing to maintain anonymity, see https://www.aljazeera.com/features/2021/5/20/the-child-victims-of-the-uks-encrochat-house-raids Abbas Nawrozzadeh also mentions in his piece that "there will be lawyers who have used Encrophones to communicate with their clients.", see https://www.aljazeera.com/opinions/2020/7/25/the-encrochat-police-hacking-sets-a-dangerous-precedent. This is confirmed by this article which reports that lawyers in Sweden used EncroChat https://www.svt.se/nyheter/har-lacker-advokaterna-hemlig-information-till-varbynatverket (in Swedish).

33 In an expert legal opinion, Lord David Anderson QC warned the Crown Prosecution Service that "the arguments for unlawfulness are formidable". Lord Anderson found it striking that not a single user was identified in the EncroChat warrant, and that UK law enforcement was "seeking to set aside the statutory requirement of an identified and circumscribed criminal enterprise in favour of a wholly general attempt to uncover serious criminality of all kinds". This expert opinion was never disclosed to defence lawyers in UK criminal cases. https://www.computerweekly.com/news/252500061/EncroChat-Top-lawyer-warned-CPS-of-risk-that-phone-hacking-warrants-could-be-unlawful Objections against the legality of the EncroChat bulk interception have also been raised in France, see https://www.computerweekly.com/news/252499785/French-legal-challenge-over-EncroChat-cryptophone-hack-could-hit-UK-prosecutions

34 Processing information obtained in bulk without proper documentation of its source could also reduce the evidential value in criminal proceedings of the information distributed by Europol to Member States' authorities. A Swedish court of appeal found "ambiguities" in the evidence from the EncroChat operation and overturned a conviction based on that evidence.

Further, Europol can become a vehicle of forum shopping[35] in cross-border cases if extremely intrusive investigative measures such as bulk hacking are carried out by authorities in a Member State whose national law permit this, and the information obtained is subsequently distributed ("attributed") to all other Member States through Europol's analysis of large data sets.

Irrespective of the issue of forum shopping, Europol should only be allowed to process large data sets obtained from Member States or other sources if the initial data collection is subject to sufficient safeguards to ensure that interferences with fundamental rights are limited to what is strictly necessary. Such limitations and safeguards, however, are completely missing from the Commission's proposal.

The proposed data-mining powers for Europol raise doubts as to whether the amount of collateral intrusions could soon reach disturbing levels in the context of bulk data interception operations similar to the EncroChat case. Such interception or data collection could potentially affect persons whose communications are protected by immunities and legal privileges under the domestic laws of the State where they reside (like lawyers, doctors and journalists). As a result, the fundamental rights at stake are not restricted to the right of data protection and right to privacy, but also include the right to a fair trial, media freedoms and freedom of expression, as surveillance can deter speech.

EDRi's analysis of some forms of mass surveillance practices (specifically biometric mass surveillance) has demonstrated the significant undue interference in a wide range of fundamental rights which can arise from indiscriminate/mass surveillance.[36] Purportedly 'targeted' surveillance practices (which in and of themselves can threaten fundamental rights protections, for example in the discriminatory ways in which certain groups are unfairly and disproportionately targeted by state surveillance) can also function as a trojan horse for practices that may, in fact, constitute mass surveillance. Such practices claim to be limited and proportionate when in fact they are fundamentally wide-ranging and indiscriminate in nature.

1.2 "Exceptional" analysis of large data sets will likely not be the exception

Based on its analysis of the EDPS Decision on Europol's "big data challenge", the Commission proposes new legal grounds for information processing in Article 18 paragraph 5a and Article 18a. Article 18, new paragraph 5a gives a legal basis for the "temporary processing" of personal data to check if it is in line with Europol's mandate, while Article 18a permits the processing of personal data in "exceptional cases" to support a specific criminal investigation.

First, what is definitely unclear is the relationship between the two Articles. The Commission's impact assessment reads as follows: the initial processing might be carried out "in case of doubts and prior to any further data processing".[37] Which means that this initial processing is not always required. Paragraph 5a adds

https://www.computerweekly.com/news/252500524/Swedish-court-finds-ambiguities-in-hacked-EncroChat-cryptophone-evidence

35 "Forum shopping" is a term used to describe a situation in which a national law enforcement authority chooses to collect evidence in another jurisdiction which has a lower level of human rights safeguards or allows for more intrusive methods.

36 EDRi, *Ban Biometric Mass Surveillance*, May 2020, available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

37 European Commission, *Impact Assessment Report*, SWD(2020) 543 final, part 1/2, page 50

that the Management Board "shall further specify the conditions relating to the processing" of the data on a proposal of Europol's Executive Director and after consulting the EDPS. It is unclear if such "conditions" refer to the "temporary" processing or the processing foreseen under Article 18a. While EDRi advises against introducing any derogation to Europol's current mandate, further clarification should be at least given as to when (the circumstances and conditions) Europol is required to check that it does not illegally process data.

Second, paragraph 1(b) of Article 18a effectively gives Europol the option to exempt itself (derogate) from the data protection rules in Annex II when analysing investigative case files provided by Member States or the EPPO. The only condition for this derogation is an assessment by Europol itself that complying with data protection requirements in Annex II will make it impossible to carry out the operational analysis.

Following its inspection, the EDPS noted that "the processing of large datasets has become an important part of the work performed by Europol to produce "criminal intelligence" and support Member States' law enforcement authorities".[38] Europol also informed in its 2019 Annual Activity Report that "the volume and complexity of the data per contribution increased considerably as big data dumps of multiple terabytes per investigation are becoming the standard procedure."[39] There is unfortunately no statistical data or numbers provided by the European Commission in its impact assessment in order to get a clearer picture about the frequency with which Europol receives that kind of material and the significance of the trend.[40] However, the EDPS' observation calls into question the European Commission's assessment that this practice would remain exceptional and that the derogation to fixed rules in the Regulation would be strictly limited and controlled.

Furthermore, Article 18a (1)(b) gives the responsibility to Europol itself to assess the necessity and proportionality of the processing of information and whether it is inevitable or not. It is hard to imagine that Europol would decide against its own operational interests and assess in an impartial manner the necessity and proportionality to process personal data that in ordinary times it should not even store.

It is important to stress that the impact assessment depicts the issue as a "lack of clarity" when actually the current legislation is perfectly clear about the prohibition for Europol to process data outside of the list established in Annex II.[41] Instead, there is a lack of legal basis for Europol to process data related to persons who are not related to a crime. EDRi believes this restriction should be strictly maintained in order to respect the principle of proportionality, given the intensity of the interference with fundamental rights such measure would entail. Data protection rules and fundamental rights safeguards will be completely undermined if Europol can simply choose to ignore them whenever they restrict Europol's operational analysis activity.

38 European Data Protection Supervisor, 'Invitation to the Seventh JPSG meeting on 28-29 September 2020', available at: https://www.europarl.europa.eu/cmsdata/211695/EDPS_letter_23092020.pdf

39 Europol, *Consolidated Annual Activity Report 2019*, 2 July 2020, available at: https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2019

40 The Impact Assessment (part2/2) only provides numbers extracted from Europol's Consolidated Annual Activity Reports, that lay down the numbers of operational cases supported and reports produced by the various specialised internal units without indicating whether it involved the processing of large datasets. Paragraph 37 of the proposal amends Article 51 of the Europol Regulation by introducing the transparency requirement to release the number of instances where Member States requested Europol to analyse large and/or complex data sets, and the number of time, but these numbers should be already available as the practice already regularly happens and as evidence to motivate the legislative reform.

41 European Commission, *Impact Assessment Report*, SWD(2020) 543 final, page 68. This is also incontestable when reading Article 18(2)(a) of the Europol Regulation.

However, this type of legal circumvention is precisely what the Commission proposes in Article 18a.

Arguably, the risk that the Commission depicts in its evaluation of policy option 5 (i.e. allowing Europol to process data from individuals not related to a crime in a structural and permanent manner) that the general public's perception of the Agency would be altered and deteriorate is substantial, even in case of exceptional derogation from fixed rules. The storage of innocent persons' data (and possibly sensitive communications content or metadata of people with protected status) for months or even years (the foreseen retention period covers the criminal investigation and the subsequent judicial proceedings) in Europol's databases, simply because their data was caught in the same net as suspects of crime, will only exacerbate Europol's reputation as a powerful yet opaque and unaccountable agency.

2. The reform of Europol's mandate should be an opportunity to question the rise of Big Data and mass surveillance in law enforcement

The proposal reflects the general and growing efforts by law enforcement authorities in developing and deploying ever more intrusive investigation tools in order to investigate illegal activity and prosecute criminals. Where the data needed to incriminate a suspect or to serve as evidence in judicial proceedings is difficult to access (most often due to the use of encryption), the recourse to hacking techniques is increasingly common among investigative authorities. This is evidenced by the recent adoption in several EU Member States of specific legislative provisions to legalise hacking practices.[42] Hacking techniques are considered extremely invasive because law enforcement can gain access to a much greater amount of data than traditional investigative tools (all data held on a device, as well as all information flows in and out of the device) but also to extremely sensitive data.[43] In that regard, the American Civil Liberties Union stressed that "the use of malware and zero-day exploits is more invasive than other forms of permissible searches because the consequences and collateral damage associated with their use are inherently unpredictable and often irreversible".[44]

Consequently there are significant human rights challenges attached to the increasing reliance on invasive surveillance activities, notably the severe restrictions they place on privacy. From a fundamental rights perspective and with due regard to the principles of necessity and proportionality, it is highly problematic that numerous national laws allow the use of advanced technical means for mass surveillance in which an unspecified number of devices can be investigated and innocent users may be impacted.

---

42 France, Poland, the UK, the Netherlands, Sweden and Italy have introduced such specific legislative frameworks from 2015 to 2020. See M. Gutheil, Q. Liger, A. Heetman, J. Eager, M. Crawford, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, IPOL_STU(2017)583137, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf
See E. Skoglund, 'Swedish law enforcement given the permission to hack', 26 February 2020, available at: https://edri.org/our-work/swedish-law-enforcement-given-the-permission-to-hack/

43 M. Gutheil, Q. Liger, A. Heetman, J. Eager, M. Crawford, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, IPOL_STU(2017)583137, available at:https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

44 ACLU, *Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media*, 31 October 2014, available at: https://www.uscourts.gov/sites/default/files/2014-11-criminal-public-hearing-testimony.pdf

It also negatively impacts judicial oversight as it was reported that the judiciary across several Member States is lacking crucial knowledge on the surveillance techniques they are authorising, including the magnitude and seriousness of their potential consequences.[45] Therefore, data from Member States that do not ensure a high level of fundamental rights protection should not be entered in EU systems that enable Member States to take action on the basis of such data.

Beyond these mass surveillance techniques rolled out by national authorities, private actors have also identified law enforcement demands for more data and information (and the convenient processing software included in the sales pack) as a profitable market. The way those profit-seeking companies are collecting personal data to make it available to law enforcement is often neither transparent nor legal, leading to recent controversies.[46]

Given that Europol's work rests upon the activities of national law enforcement agencies and the data they gather, the expansion of its already extensive powers to massively collect, store and analyse information on individuals should be examined as part of the critical reflection on today's electronic mass surveillance. More generally, this issue of Europol's "big data challenge" brings into question the mass surveillance and bulk processing of people's personal data by law enforcement and other security authorities. The evolution of the agency's role and importance in the processing and analysis of large datasets has not arisen in a void. Questioning the provenance of data used for mass processing is fundamental to holding law enforcement accountable and safeguard fundamental rights.

2.1 The role of Europol in AI-based and data-driven policing should be assessed

The use of Artificial Intelligence (AI) solutions and data-driven tools in the field of law enforcement and criminal justice systems is becoming a reality in Europe, yet the particular high risks of violations and limitations of fundamental rights are insufficiently addressed in ongoing debates at EU level as well as in the recent proposal for an Artificial Intelligence Act by the European Commission in April 2021.

In recent years, we observed an increased, yet un-evidenced, narrative of the feasibility of "predicting" and "preventing" crime using data driven tools; and an increase in volume and complexity of data that necessitates the use of more sophisticated analysis tools.[47] In the context of the reform of Europol's mandate, the apparent need for Europol to analyse large datasets is similarly explained by two factors: (1) not all Member States possess the IT tools, expertise and resources to use sophisticated technologies for predictive policing and data mining on their own; and (2) because of this lack of resources, those Member States started submit-

45 M. Gutheil, Q. Liger, A. Heetman, J. Eager, M. Crawford, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, IPOL_STU(2017)583137, available at:https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

46 Clearview AI has been one of most recent scandals (See E. Jakubowska, Stalked by your digital doppelganger?, 29 January 2020, available at: https://edri.org/our-work/stalked-by-your-digital-doppelganger/), as well as Banjo (See J. Cox and J. Koebler, 'Surveillance Firm Banjo Used a Secret Company and Fake Apps to Scrape', *VICE*, 9 March 2020, available at: https://www.vice.com/en/article/z3bgky/banjo-ai-used-secret-company-and-fake-apps-to-scrape-facebook-twitter)

47 A. Babuta and M. Oswald, *Data Analytics and Algorithms in Policing in England and Wales Towards A New Policy Framework*, Occasional Paper, Royal United Services Institute for Defence and Security Studies, February 2020, available at: https://rusi.org/sites/default/files/rusi_pub_165_2020_01_algorithmic_policing_babuta_final_web_copy.pdf

ting "large and unfiltered datasets" to Europol and delegating parts of their operational work to the Agency (which is not an ordinary police authority with operational powers), despite the absence of a legal basis for taking such an action.[48]

A recent study, commissioned by the European Parliament Think Tank at the request of the Civil Liberties, Justice and Home Affairs Committee (LIBE), explains the worrying absence of debate by the fact that the regulation of AI has primarily been developed from the primary perspective of the Digital Single Market, with economic considerations at the center of the discussion. The study emphasises that "the current EU data protection legal framework shall not be assumed to offer enough solid safeguards for individuals in light of the increased uses of automated decision-making and profiling for law enforcement and criminal justice purpose" and "recommends that due consideration be given to the need for a legislative intervention to guarantee EU fundamental rights in the field of law enforcement and criminal justice".[49]

Indeed, a wide range of fundamental rights are impacted by the introduction of AI systems and algorithms in the field of law enforcement, including privacy and data protection rights, procedural rights (i.e. right to fair trial, right to an effective remedy) but also the right to non-discrimination. In particular, big data and algorithmic systems rely on the prioritisation of certain values or characteristics which can be motivated by racialised assumptions and other discriminatory practices or actions. Regardless of whether Europol uses sophisticated analytical tools (e.g. AI-based) or not when analysing large volumes of information, it cannot be excluded that the outcomes of this analysis may have disproportionate impacts on racialised and marginalised groups. As demonstrated in a 2019 report from the European Network Against Racism (ENAR), "the presence of new technologies both assists and drives over-policing by providing law enforcement agencies with risk-making capabilities, alongside developing databases which contain racialised stereotypical assumptions of minority communities."[50]

This can be linked to the nature, source or composition of the datasets transferred by Member States, basically consisting of "dirty data" ("data that is distorted by individual and societal biases" or data emanating from "corrupt, biased, and unlawful practices", see paragraph 2.1. above).[51] Or it could be explained by Europol's "digital forensics" methods themselves, whereby certain criteria translating existing prejudice overly flag individuals from certain socioeconomic, racial or ethnic groups. This prejudiced identification can result in these individuals being placed under further investigative scrutiny or other coercive measures by decision of a Member State authority. The EDPS also pointed to the risk in its decision that the analytical process applied is leading to the "loss of technical and factual context" and to "increased bias".[52] In that regard, the European Commission failed to identify the fundamental right to non-discrimination as potentially impacted by these

48 European Commission, *Impact Assessment Report*, SWD(2020) 543 final

49 Prof. Dr. G. González Fuster, *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, IPOL_STU(2020)656295, available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)656295

50 ENAR, *Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe*, November 2019, available at: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf

51 Richardson, R., J. Schultz and K. Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations*, New York University Law Review Online 192, 13 February 2019, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423

52 EDPS, 'Decision on the own initiative inquiry on Europol's big data challenge', 18 September 2020, available at: https://www.statewatch.org/media/1397/eu-edps-decision-redacted-inquiry-europol-big-data-challenge-10-20.pdf

new provisions (while it did for the processing of data for the purposes of research and development).[53] This oversight, alongide a low level of democratic oversight and accountability[54] (see 2.2. below), has led to a gravely inadequate mitigation of the potential fundamental rights violations in relation to Europol's data processing activities and computer-assisted investigative techniques.

The proposal would give Europol the ability to continue this work, "including for preventive action and criminal intelligence"[55], without assessing its current techniques or enabling their proper democratic scrutiny. The European Parliament should require the assessment of Europol's current analytical methods and how they affect national law enforcement decisions and activities.

2.2 Oversight mechanisms should be strengthened

The proposed updates to the Europol Regulation would create far-reaching new data-processing capabilities for Europol. Yet there is no indication in the Commission's proposal that the current oversight mechanisms will be adapted or meaninfully strengthened in response to this expanding mandated. The Commission only proposes an obligation on Europol to extend existing reporting obligations "in the necessary confidentiality" to the European Parliament by adding slightly more information illustrating its annual activities. There is nothing to suggest there will be proper scrutiny of Europol's current operational work and its compliance with applicable rules.

The 2016 Europol Regulation provided a scrutiny mechanism by establishing a Joint Parliamentary Scrutiny Group (JPSG), composed of Members of the European Parliament (MEPs) and national Parliaments. Strong concerns were already voiced with regards to the applicability of the current mechanism.[56] Parliamentary oversight and access to information provided for by the Regulation remain superficial as they do not apply to Europol's day-to-day work. Europol is rarely subject to significant scrutiny of the administration and organisation of its work, in particular its operational work. The European Parliament should demand as part of the legislative process that:

- An evaluation of the work of the JPSG is carried out in order to determine whether or not it has been able to carry out its missions before the new mandate is adopted;
- The future Europol regulation provides the JPSG with real powers of supervision by:
  - Enabling the scrutiny of Europol's day-to-day work and the issuance of binding recommendations;
  - Granting it decision powers in the appointment of the Executive Director and its Deputy Directors;
- An evaluation of the possibility of granting the JPSG voting rights in Europol's Management Board.

The fact that Europol is using the software of the US big data analytics firm Palantir for "the operational analysis of all counter-terrorism related data" – a company which has been involved in data scandals; and criti-

53 European Commission, *Impact Assessment Report*, SWD(2020) 543 final
54 Europol had to signal itself that there was a legality issue about some of its ongoing data processing activities. See footnote 21
55 European Commission, *Impact Assessment Report*, SWD(2020) 543 final, page 41
56 M. Monroy, 'Oversight of the new Europol regulation likely to remain superficial', 12 July 2016, available at: https://edri.org/our-work/oversight-new-europol-regulation-likely-remain-superficial/

cised for cooperation in deportations with the US Immigration and Customs Enforcement[57] and its close ties to far-right politicians across the globe - was only made public and known to MEPs recently.[58] MEPs are forced to request this type of information as their scrutiny abilities do not include the review of computer-assisted investigative techniques and how they function. The extension of the supervision mandate of the JPSG as outlined above should address this issue and increase its ability for effective oversight.

Europol's role in research and innovation: the quest for new and shiny policing tools

- Data protection rights of affected data subjects should be upheld by prohibiting measures and decisions that might affect the data subjects not just linked to the personal data processed but also to the subsequent use of the algortihms produced.
- The national Data Protection Authorities under the coordination of the European Data Protection Board (EDPB) should conduct an examination of the impact on all fundamental rights as result of data transfers by Member States to Europol as well as their legality.
- Europol should not be given any meaningful decision-making role in the management of EU security research programmes as it would deepen the democratic deficit of the EU's actions in this field.
- EDRi recommends to delete Article 33a and Article 18 (2)(e). If pursued nonetheless, the following safeguards should be put in place:
- (1) establishing a strong review and scrutiny process with affected groups and democratic representatives, notably the JPSG;
- (2) proscribing any research project of which the outcomes would result in fundamental rights abuses – notably the right to non-discrimination - or systematic harm to individuals, communities and societies;
- (3) imposing regular, comprehensive human rights impact assessments;
- (4) ensuring a high level of transparency by requiring the publication of the project's description, testing methods and human rights impact assessments.

1. Opaque and unaccountable algorithmic experiments will not improve people's trust in Europol

> *"Lack of transparency can dramatically affect the trust of the population in the role of the EU in supporting AI in law enforcement and criminal justice." - Prof. Dr. Gloria González Fuster*

EU law enforcement bodies have invested resources to take advantage of new technologies for policing purposes. In this context, the Commission's proposed reform is to formalise Europol's role in EU's research and

57 Mijente, 'Who's Behind ICE? The Tech and Data Companies Fuelling Deportations', 23 October 2018, available at: https://mijente.net/2018/10/whos-behind-ice-the-tech-companies-fueling-deportations/

58 C. Ernst, 'Palantir software at EU agencies', Parliamentary Question, 25 September 2020, available at: https://www.europarl.europa.eu/doceo/document/E-9-2020-000173_EN.html

development (R&D) initiatives and reinforce its own "research and innovation" capacities. It would enable Europol (1) to support the Commission in the implementation of Union framework programmes for research and innovation activities that are relevant for law enforcement; (2) to continue the activities of the existing innovation lab; (3) to support the EU innovation hub for internal security; as well as (4) to process personal data, including high volumes of personal data, for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement.

The reinforcement of Europol's role in security research takes place in the wider EU project of creating a "European Security Data Space". The idea is to set up a "common data platform with trusted datasets to train, test and validate algorithms, with the purpose of creating sufficient quantity of high quality and reliable data to research and develop Artificial Intelligence technologies in the domain of law enforcement."[59]

Regarding the "Europol Innovation Lab", it was established in May 2020 following the conclusions of the Justice and Home Affairs (JHA) Council, calling for Europol to actively "monitor [...] new technological developments and drive innovation, including by developing common technological solutions for Member States in the field of internal security."[60] More recent discussions foresee the development of a EU Innovation Hub for Internal Security in the coming months, which would not solely serve the interest of the law enforcement community (like the Lab does), but of the "wider field of internal security, including border management, criminal justice and the security aspects of migration and customs".[61]

Once more, the first objective of the revision of Europol's mandate is to give legal footing to what was already developed and is already taking place on the sole basis of political decisions, thus excluding any possibility to organise a wider democratic debate. As expected by the Commission, the legal basis should also bring adequate funding to the four functions for the Lab: 1) the Projects in which EU Member States develop "innovative" tools and provide solutions to serve the operational needs of law enforcement, 2) the Observatory tasked with producing assessments on the risks, threats and opportunities of emerging policing technologies, 3) the Network of Innovators including the industry, civil society, international organisations and academia, and 4) the EU Innovation Hub for Internal Security (a distinct entity from the Lab but hosted at the Lab). In this framework, Europol would, among other tasks, monitor the emergence of new technologies for law enforcement purposes, support Member State's work in research and development, implement its own "innovation projects" ("covering notably the uptake of applied research towards deployment, and the work towards a final product available for the use by law enforcement"[62]) and support the uptake of the results of "innovation projects".

59 DG Migration and Home Affairs, *Management Plan 2020*, available at: https://ec.europa.eu/info/system/files/management-plan-home-2020_en.pdf
European Commission, *Communication on the EU Strategy to tackle Organised Crime 2021-2025,* available at: https://ec.europa.eu/home-affairs/sites/default/files/pdf/14042021_eu_strategy_to_tackle_organised_crime_2021-2025_com-2021-170-1_en.pdf

60 Europol, 'Written contribution to JPSG. The Europol Innovation Lab', 28 May 2020, available at: https://www.europarl.europa.eu/cmsdata/208046/Europol%20Contribution%20for%20Electronic%20exchange%20-%20Europol%20Innovation%20Lab.pdf

61 Council of the European Union, 'The EU Innovation Hub and the Innovation Lab of Europol –state of play,' LIMITE 12859/20, 16 November 2020, available at: https://www.statewatch.org/media/1474/eu-council-europol-innovation-lab-update-12859-20.pdf

62 European Commission, *Impact Assessment Report*, SWD(2020) 543 final, page 53

1.1 Data protection rights of affected data subjects should be upheld

In the context of its "research and innovation" projects, Europol would be using the large datasets at its disposal, including operational data. The impact assessment informs that only "personal data that fall into one of the data categories of Annex II of the Europol Regulation, i.e. personal data that is linked to a crime" would be processed.[63] The use of "real data" is justified by the requirement to build "algorithms [which can] produce results that are sufficiently precise."[64] The list of safeguards foreseen includes: the prior authorisation by Europol's Executive Director, the prior information of the EDPS and the Management Board, the separation of research data from the rest of Europol's operational data with controlled and restricted access, the protection of data subjects concerned against measures or decisions affecting them as a result of the project, a retention period and the conservation of processing logs in order to verify the accuracy of the outcome.

More detailed data protection safeguards are mentioned in the impact assessment, notably limiting the "processing to what is strictly necessary for a specific purpose, e.g. processing anonymised and pseudonymised data for the development of algorithms."[65] It is EDRi's opinion that the anonymisation of all operational data that are used for the purpose of "research and innovation" would be a good standard practice to ensure the EU data protection principles are respected in the context of these projects, such as purpose limitation, data minimisation, privacy by design and by default, etc. Ideally, anonymisation should be a legal requirement in Article 33a in order for Europol to use its operational data for research and innovation projects. However, as stressed by the EDPS in its opinion on the European Strategy for Data, "anonymization processes are not straightforward. The more varied the data, the more difficult it is to be anonymised by reducing the re-identification risk to an acceptable threshold."[66] To achieve anonymisation under GDPR and data protection rules for EU institutions, re-identification of a data subject (even by the controller that anonymised the data) must be impossible with all means reasonably likely to be used.[67] Since Europol generally retains access to the original data set for operational purposes, the risk of re-identification of the data subjects in the research data set can only really be migitated through strict organisational safeguards (as Article 33a(1)(c) seeks to achieve). A technical protection against re-identification will require research projects to be restricted to using aggregated and anonymised data.[68] **If anonymisation is carried out, the data protection impact assessment should take into due account the risk that the selected data could be paired with other available information to deduce the identity of data subjects.**

Furthemore, recital 39 of the proposal explains that Europol should first carry out an assessment of the impacts on fundamental rights before starting the processing operations. This should include an assessment of the "appropriateness of the personal data" chosen to be processed for the project. However, it is unclear ac-

63 Idem, page 55
64 Idem, page 75
65 Idem, page 77
66 EDPS, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, page 8, available at: https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf
67 Recital 16 of Regulation (EU) 2018/1725 and recital 26 of the GDPR.
68 In some cases, differential privacy techniques could potentially be used to irreversibly break any links between the research data and the original personal data (still retained by Europol for operation purposes) and thus prevent re-identification of data subjects. See this Access Now explainer on differential privacy: https://www.accessnow.org/understanding-differential-privacy-matters-digital-rights/

cording to which criteria the data will be selected and how the level of "appropriateness"- which, unlike necessity and proportionality, is not a legal standard - will be measured. It is also questionable that Europol has the capacities and legitimacy to carry such necessity (Article 33a(1)(a)) and proportionality assessment.

The proposal gives the responsibility to evaluate the impacts of the "research and innovation" projects on data protection to Europol itself. Article 33a (1)(a) of the proposal puts Europol's Executive Director in charge of authorising the processing activities based on a description and a data protection impact assessment provided by Europol's internal operational units. The EDPS is only "informed" prior to the launch (Article 33a (1)(b)) and can exercise its corrective powers on the basis of Europol's assessment, including potentially a prohibition of the processing. It should be clarified in the operational part of the Regulation that Article 39 of Europol's Regulation[69] relating to the prior consultation of the EDPS applies for all "research and innovation" projects.

Furthermore, the safeguard according to which personal data processed in the context of the research project cannot be used to take measures or decisions affecting the data subjects, does not prevent Europol from using algorithms developed in the research project for similar measures or decisions affecting the same group of individuals. Algorithms will often reflect and could contain the same assumptions and potential biases as the underlying (training) dataset. **We therefore recommend to prohibit measures and decisions linked to the subsequent use of the algortihms produced that might affect the data subjects.**

1.2 The strategic selection and promotion of research projects implying high risks for fundamental rights should not be the responsibility of an unaccountable EU agency

The new mandate would also foresee a role for Europol in identifying research priorities to which EU funds should be allocated, notably as part of the Union framework programmes (like Horizon Europe). Actually, Europol is already involved in nationally-funded and EU-funded research projects, via the Horizon 2020 research and innovation budget. The agency currently participates in three EU-funded research projects (AIDA, GRACE and INFINITY), looking into the use of artificial intelligence, big data, machine learning and virtual and augmented reality for law enforcement purposes.[70]

First, Europol's role in setting priorities for EU funding raises a clear concern as to democratic oversight insofar as it constitutes a process of influencing research and development priorities of Member States. Second, the opacity and the lack of accountability and democratic oversight of EU funding in the field of "research and innovation" related to law enforcement and criminal justice have already been identified as significant problems in a study conducted for the European Parliament.[71] Involving an EU agency that is unaccountable, opaque and not subject to adequate parliamentary scrutiny or judicial oversight would further accentuate the existing problematic lack of minimum transparency standards and independent oversight. This is why we strongly advise against giving Europol a more prominent role in determining EU research and innovation

69 Including the consultation process described in Article 90 of Regulation 2018/1725

70 Statewatch, 'EU: Police seeking new technologies as Europol's "Innovation Lab" takes shape', 18 November 2020, available at: https://www.statewatch.org/news/2020/november/eu-police-seeking-new-technologies-as-europol-s-innovation-lab-takes-shape/

71 Prof. Dr. G. González Fuster, *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, IPOL_STU(2020)656295, available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)656295

funding priorities.

The selection of law enforcement-related research projects at EU level has the potential to dramatically affect future policing practices with considerable consequences on the lives and rights of persons subject to them. The risks are manifold: the projects' outcomes could lead to the deployment of unlawful biometric mass surveillance systems[72] or to the use of 'predictive' algorithmic systems by national and local police officers that codify racialised assumptions and other systematic discrimination and violence.[73]

> *"Increasing evidence demonstrates how emerging technologies may not only exacerbate existing inequalities, but in effect differentiate, target and experiment on communities at the margins – racialised people, undocumented migrants, queer communities, and those with disabilities" - Sarah Chander, EDRi Senior Policy Advisor*[74]

It is essential to ensure that Member States cannot use the resulting technologies in a way which gives way to fundamental rights abuses. Yet, the level of involvement of democratically elected bodies in setting the priorities, overseeing the spending of EU funds and thus, preventing rights violations or harms, remains critically low. **EDRi believes that Europol should not be given any meaningful decision-making role in the management of EU security research programmes as it would deepen the democratic deficit of the EU's actions in this field.**

2. Technological sovereignty and 'de-biasing' should not be used as red herring

> *"[The European Commission is] proposing that Europol develops new technologies using vast quantities of personal data gathered by the very institutions that engage in discriminatory practices. Will that really help meet the [EU Anti-Racism] Action Plan's goal of "doing more to tackle racism in everyday life"?" - Statewatch*[75]

The proposal to increase Europol's responsibility in the field of security research also implies the task to help screening "specific cases of foreign direct investments that concern contract providers of technologies and software for police forces". The attribution of this task to Europol is motivated by the ambition to "strengthen technological sovereignty and strategic autonomy of Member States of the EU in the area of internal security", and so is the mission to develop and validate AI-based policing tools too.[76] The Commission's impact assessment provides further insight into this underlying motivation: "It would reduce the dependency on products that were developed outside the EU, which might be developed based on different data, according to different rules, and with different objectives, and hence not necessarily in a transparent way that complies

72 EDRi, *Ban Biometric Mass Surveillance*, May 2020, available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

73 S. Chander, 'Technology has codified structural racism – will the EU tackle racist tech?', 3 September 2020, available at: https://www.euractiv.com/section/digital/opinion/technology-has-codified-structural-racism-will-the-eu-tackle-racist-tech/ EDRi, *Structural Racism, Digital Rights and Technology,* July 2020, available at: https://edri.org/wp-content/uploads/2020/09/Structural-Racism-Digital-Rights-and-Technology_Final.pdf

74 Idem

75 Statewatch, 'Big data experiments: new powers for Europol risk reinforcing police bias', 11 February 2020, available at: https://www.statewatch.org/news/2021/february/big-data-experiments-new-powers-for-europol-risk-reinforcing-police-bias/

76 European Commission, *Impact Assessment Report,* SWD(2020) 543 final, page 55, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate

with EU norms and Fundamental Rights. It would therefore reduce the risk of biased and thus inaccurate outcomes, which in turn reduces the risk of discrimination."[77]

EDRi believes this is a highly contestable and dangerous rationale which undermines the crucial wake-up call from several civil society groups that asssitive technologies for policing exacerbate existing inequalities and further criminalise racialised, marginalised and poor communities, regardless where they have been developed.[78] The assumption that if the creation and adoption of such technologies is a purely European process, the risks of increased discrimination and rights violations will automatically be lowered, or even become insignificant, is simply wrong.

> *"We shouldn't see the issues of the potential harmful impact on racialised communities through tech as a U.S. issue. It's going to be wherever you find manifest structural discrimination and racial inequality." - Sarah Chander, EDRi Senior Policy Advisor*

A report published by the European Network Against Racism (ENAR) on data-driven policing in 2019 rightly recalls that "technology does not simply come into existence, immaculately conceived and purposeless. Instead it is a product of its time, with all the political and social influences this brings."[79] European police forces are not exempted from racialised assumptions of suspicion, risks and criminalisation. The report highlights the overwhelming evidence of today's discriminatory policing against racialised minority and migrant communities across Europe. It then shows how such discriminatory policing is translated in technology design and development processes. When "companies design technology with specific purposes in mind, such as solving a specific 'crime' challenge, possibly for a police client, [they] inevitably [incorporate] many of the client's ideas and assumptions".[80] As a result, the technologies perpetuate pre-existing human biases, the biased corporate memory of the police and law enforcement agencies and thus, social inequalities. These risks are especially present in Europol's own "innovation projects" as the proposal would allow the use of the Agency's operational data that it has hoovered up from the Member States and third countries, carrying the legacy of their racist policing practices.

The Commission's justifications cast a huge doubt on whether EU institutions will take the necessary measures to regulate and implement adequate fundamental rights safeguards that address the harms at stake in the Europol's Regulation and other EU instruments. For example, whilst the Commission's proposal for an Artificial Intelligence Act (AIA) takes some steps to regulate the use of AI in policing – including a partial prohibition on real time remote biometric identification in publicly accessible spaces (article 5(1)(d)) and the classi-

77 Idem, page 74
78 ENAR, *Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe*, November 2019, available at: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf;
F. Jansen and S. Chander, 'Why EU needs to be wary that AI will increase racial profiling', 19 April 2021, available at: https://euobserver.com/opinion/151556;
Amnesty International, *Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database*, 23 November 2018, available at: https://www.amnesty.org.uk/trapped-gangs-matrix
79 ENAR, *Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe*, November 2019, page 14, available at: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf
80 Idem, page 14

fication of various uses of AI in law enforcement as "high risk" (Annex III), such steps are insufficient to protect against the vast range of fundamental rights risks at stake.[81] In particular, the weak procedural requirements on AI developers to examine possible bias (AIA Article 10) and to self-assess conformity with the requirements (AIA Article 43(2)) and the limited obligations on users of such systems (AIA Article 29), demonstrate an intent to facilitate and enable the use of AI systems by law enforcement. What these proposals fail to address is that, in a world of deeply embedded discrimination, certain technologies will, by definition, reproduce broader patterns of racism. **The national Data Protection Authorities under the coordination of the European Data Protection Board (EDPB) should conduct an examination of the impact on all fundamental rights as result of data transfers by Member States to Europol as well as their legality.**

Acknowledging the risks of discriminatory "biases in the operational data used for the development of algorithms" and "abuses in the application of and output from algorithms",[82] the Commission outlines a series of safeguards in its impact assessment, which are unfortunately poorly reflected in the actual text of the proposal. Article 33a (1)(a) gives the responsibility to Europol's operational unit in charge of the research project to produce a "a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks". This material would be used by Europol's Executive Director as a basis to authorise or not authorise the project.

First, it is very doubtful that Europol's staff alone has the ability to provide an accurate, impartial and fair assessment of the project, considering their own operational interests. Given the scale of the datasets under discussion (potentially involving millions of individuals) and their unique provenance (primarily coming from law enforcement agencies), it may prove difficult to accurately assess the extent of the bias involved and to find a suitable yardstick against which to measure the accuracy of the results.

EDRi believes that if Europol was allowed to conduct its own development and testing projects (which EDRi fundamentally opposes), the active and ongoing involvement of the JPSG should be required at the very least, in order to establish a minimum level of democratic scrutiny and control. The JPSG should be constantly informed of the launch of new projects and their objectives, as well as regularly updated of their advancement. In case the deliverables resulting from a certain selected project would imply high levels of intrusion, fundamental rights abuses or systematic harm to individuals, communities and societies, the JPSG should have the power to dismiss, suspend or ultimatively terminate an ongoing project. This decision should be taken on the basis of a human rights impact assessment produced by relevant stakeholders and experts depending the objectives of the project at issue: for example the Fundamental Rights Agency (FRA), the EDPS, Europol's Data Protection Officer and expert committees designated by the JPSG and composed first and foremost of

81 EDRi, 'EU's AI proposal must go further to prevent surveillance and discrimination', 28 April 2021, available at: https://edri.org/our-work/eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination/

82 European Commission, *Impact Assessment Report,* SWD(2020) 543 final, page 76, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate

representatives of groups and communities who will likely be affected by the proposed AI systems or technological solutions as well as other relevant civil society organisations. The time allocated to this assessment process should be sufficient and adapted to the stakeholders involved and proportionate to the complexity of the intended project. The process would ensure that no EU funds or research operations are allocated to the development and deployment of unacceptable AI applications, which are incompatible with fundamental rights, fundamental European values, and existing European law.[83]

Second, the Commission suggests as a safeguard to introduce measures to mitigate the potential biases in the law enforcement data and the algorithms' outputs/applications. It is not specified what kind of measures exactly it would entail but this suggestion hints towards specific technical approaches often called "debiasing". However, these techniques and processes are generally immature, are often not ready for application and their efficacy is contested.[84] Therefore, EDRi believes that relying on this exclusively technological approach would systematically fail in achieving the objective of countering discriminatory impacts.

Third, the Commission proposal's requirement to conduct a human rights impact assessment only applies prior to the project launch. We recommend that regular human rights impact assessments are performed during the development, at regular milestones, and throughout the algorithms' context-specific deployment in order to identify the risks of rights-adverse outcomes. For algorithmic systems carrying high risks to human rights, impact assessments should include an evaluation of the possible implications that these AI systems pose for existing collective, societal, institutional or governance structures.[85] Such impact assessments must be made publicly available.

Lastly, while the proposal also notes the need to "ensure transparency" (Article 33a, (3)), it is not clear whether the detailed description of the process and rationale behind the training, testing and validation of algorithms will be made public. It raises the question whether the algorithms produced by Europol will be open for anyone to inspect. EDRi supports a greater degree of transparency if Europol were to be able to conduct its own research projects by requiring the publication of the project's description, testing methods and human rights impact assessments.

EDRi therefore recommends to delete Article 33a or at least, (1) to establish a strong review and scrutiny process with affected groups and democratic representatives, (2) to proscribe any research project of which the outcomes would result in fundamental rights abuses – notably the right to non-discrimination - or systematic harm to individuals, communities and societies, (3) to impose regular comprehensive human rights impact assessments as well as (4) to ensure a high level of transparency by requiring the publication of the project's description, testing methods and human rights impact assessments.

83 EDRi, *Ban Biometric Mass Surveillance*, May 2020, available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

84 A. Balayn and S. Gürses, *Beyond De-biasing – Automated Decision Making and Structural Discrimination*, Delft University of Technology, The Netherlands (forthcoming)

85 EDRi, *Recommendations for a Fundamental Rights-based Artificial Intelligence Regulation. Addressing collective harms, democratic oversight and impermissable use*, 4 June 2020, available at: https://edri.org/wp-content/uploads/2020/06/AI_EDRiRecommendations.pdf

Easing personal data transfers between Europol and third countries

- EDRi opposes the new derogation to provisions designed to protect individual rights.
- A thorough evaluation of how and why Europol and national law enforcement authorities use the derogations currently available is required to assess the necessity and proportionality of any new derogation.

Transfers of personal data between Europol and non-EU states ("third countries") can only take place according to certain requirements, namely: the existence of a Commission adequacy decision regarding a particular state; an international agreement between the EU and a particular state permitting such transfers; or the existence of a cooperation agreement between Europol and a particular state, agreed in accordance with the agency's previous legal basis.[86] However, a derogation from these requirements is possible for certain purposes, on a case-by-case basis, in individual cases.[87] Moreover, such a derogation may be extended for a period of up to a year, with the agreement of Europol's Management Board and the European Data Protection Supervisor.[88]

One of the amendments proposed by the Commission would broaden this derogation. The current derogation permits "the transfer of personal data to third countries or international organisations on a case-by-case basis". Under the proposals, the derogation would permit "the transfer **or categories of transfers** of personal data to third countries or international organisations on a case-by-case basis" (emphasis added).

The Commission argues that the Europol Regulation should be brought into line with the Law Enforcement Directive, which contains the same wording regarding "transfer or categories of transfers of personal data". However, the Law Enforcement Directive applies to national authorities, and Europol should not be treated in the same way as those authorities, whose actions it is supposed to support and strengthen. Easing Europol's ability to exchange personal data with third countries – in particular by transferring it to third countries – would mainly appear intended to benefit third countries, not the member states, who would at most be indirect beneficiaries of such cooperation. Furthermore, as the EDPS has remarked in their opinion on the proposal, the wording "categories of transfers" is vague, giving rise to potential legal uncertainty.

The Commission's staff working document also refers to the fact that there have been significant difficulties in attempts to negotiate a number of international agreements to facilitate the exchange of personal data between Europol and key third countries. It must be noted that a number of those countries are not democracies in any meaningful sense of the word, and their law enforcement authorities are regularly accused of serious human rights abuses. Thus, if it really is that important to exchange personal data with them, an international agreement over which there is some degree of parliamentary scrutiny would be a preferable means for

86 These are set out in Article 25(1)(a), (b) and (c), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794#d1e2199-53-1
87 Article 25(5), op. cit.
88 Article 25(6), op. cit.

regulating those exchanges.[89]

The potentially broad application of this proposed additional derogation is made clear by the Commission. The annexes to the staff working document accompanying the proposal state that while the proposed derogation only "facilitates the transfer of personal data in specific situations," those "specific situations (e.g. individual investigations, imminent threat to public security) cover a large number of the operational needs of law enforcement authorities, as shown by Member State authorities' use of such derogations." This proposed new exception appears to be an attempt to establish a new rule, precisely because of the political difficulties the Commission has faced in negotiating agreements. However, derogations must remain exceptional, clearly-circumscribed and limited, with strict safeguards and oversight. New derogations to provisions designed to protect individual rights should not be introduced to make up for political shortcomings in international negotiations, particularly when – as the Commission admits – the current derogations available appear to be poorly-understood and under-used.[90]

Europol's alerts in the Schengen Information System

- Europol should not be allowed to enter alerts in the Schengen Information System, which runs counter to the treaty provisions governing the Agency and raises significant legal and human rights concerns
- The European Parliament should undertake an analysis of the legal "restrictions" that prohibit member states from entering certain information in the Schengen Information System, to determine the scale and scope of the alleged problem
- Europol should publish information on which intelligence agencies of which third countries it currently cooperates, and how it does so.

Europol is currently able to access and search data in the Schengen Information System (SIS), and to exchange supplementary data with Member States when a search leads to a 'hit'. The Commission proposes building upon these powers by giving Europol the possibility to enter alerts on non-EU citizens in the SIS, described in the proposal as alerts on "persons of interest".[91] This new measure is mostly justified by the perceived need for tracking and monitoring the movements of foreign terrorist fighters. It would formalise an existing arrangement, whereby Europol "cooperates with Member States and encourage[s] them to issue alerts," which the Commission's impact assessment says is "not transparent" and "raises legal concerns (e.g. on responsibility and liability)."[92]

89 Current priority states for signing cooperation agreements are Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey. See: Warnings over proposed new Europol partners in Middle East and North Africa, *Statewatch*, 14 May 2018; Council bypasses Parliament onEuropol personal data exchange deals with Middle Eastern and NorthAfrican states, *Statewatch*, 18 June 2018

90 European Commission, *Impact Assessment Report,* SWD(2020) 543 final, Annex 7

91 Proposal for a Regulation amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, 9 December 2020, available at: https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-791-F1-EN-MAIN-PART-1.PDF

92 An explanation of the current system is available here: Matthias Monroy, 'German proposal: Prohibited EU secret service cooperation through the back door', 20 October 2020, https://digit.site36.net/2020/10/20/german-proposal-prohibited-eu-secret-service-

Under the proposed rules, if a search in the SIS (e.g. by a border guard or police officer) triggers a "hit" against an alert entered by Europol, they would be informed that Europol holds information about that person. The frontline officer would have to report to their national SIRENE bureau, which in turn would inform Europol that the person of interest had been located and of the place, time and reason for the check. Further information could then be obtained from Europol and the national authority could decide, on the basis of national law, if any further action were to be taken against the individual.

The Commission's proposal notes that there are certain risks inherent in this approach, but the safeguards and transparency measures it offers in response are rather limited. Alerts would be limited to known criminals and suspects. The latter category is already very broad, and the proposal does not limit the scope to any particularly serious offences covered by Europol's mandate. Europol would also be required to verify that data on individuals received from third countries is reliable and accurate, but it is not clear that Europol would be capable of undertaking meaningful assessments with regard to this category of information (particularly if, as the proposal suggests, it should check with the third country itself whether the information is reliable and accurate). With this in mind, other provisions – for example, time limits for mandatory review of alerts sourced from third states, or some minor transparency measures for the European Parliament – have little to offer.

As noted above, although the existing arrangement raises "legal concerns", the proposals come with problems of their own. The proposal raises numerous, serious, legal and human rights risks: it reverses Europol's role as defined in the treaties; it gives the agency a privileged role in the surveillance of supposedly risky individuals; it seeks to leapfrog national legal requirements governing the handling of information received from non-EU states; it would intensify cooperation with countries and agencies with appalling human rights records; and it provides an avenue for the political persecution of dissidents by such countries. It is disproportionate and should be rejected.

Article 88 of the Treaty on the Functioning of European Union says that Europol's role shall be to "support and strengthen action by the Member States' police authorities and other law enforcement services" and excludes the application of coercive measures by the agency. However, the proposal would create an obligation for member states to take action based on information entered in the SIS by Europol and, in doing so, reverses this supporting role. Specifically, national authorities would have to report to Europol the person of interest had been located and the place, time and reason for the check. Beyond this explicit obligation to act at the behest of Europol, the proposal notes that there is no obligation for the national authority to take coercive action of any kind against the individual(s) who are the subject of the alert. However, the proposals would vastly increase the possibility that some form of coercive action will be taken, thus limiting the discretion of the na-

cooperation-through-the-back-door/; see also: Council of the European Union, 'Defining a process for evaluating and possibly entering information from third countries on suspected Foreign Terrorist Fighters in the Schengen Information System', document 11564/3/20 REV 3, 16 November 2020, https://www.statewatch.org/statewatch-database/council-of-the-eu-defining-a-process-for-evaluating-and-possibly-entering-information-from-third-countries-on-suspected-foreign-terrorist-fighters-in-the-schengen-information-system/

tional authorities vis-a-vis Europol. Alerts on persons in the SIS are included precisely for the purposes of prompting coercive measures. Even if there is no obligation to undertake such measures, a presumption to do so will remain.

This requirement to provide Europol with information on the place, time and reason for the check is also intended to "increase Europol's analytical capability (e.g. to establish a picture of travel movements of the person under alert), enabling Europol to provide a more complete information product to Member States." Given the risks of politically-motivated surveillance introduced by this proposal (discussed further below), this is a dangerous proposition, particularly were Europol to share data on an individual's movements with the third country that supplied the data in the first place. It also negates the fact that it is for the national authorities to determine which data should be entered in the SIS – under these proposals, national authorities would be acting on Europol's behalf.

The proposal also seeks to bypass national legal requirements regarding the handling of data received from non-EU states. The Commission says that under the current system, Member States do not always enter information received from non-EU states in the SIS – for example, because "a link to national jurisdiction" may be required (in general, such procedural requirements are referred to as "restrictions in national law"). However, there is no data on the extent of these issues, which Member States they affect, or any other detailed data. A more considered analysis of the nature of these "restrictions" and the problems they cause is required if the Commission's arguments of necessity are to be taken seriously.

Cooperation with non-EU states that have appalling human rights records would also likely increase if the proposals are approved[93] (easing data transfers with third countries is also a more general aim of the proposal, examined in the previous section). With regard to the possibility for Europol to enter its own alerts in the SIS, information on alleged foreign terrorist fighters – one of the main justifications for the proposals - is likely to be received from intelligence agencies. While Europol is not prohibited from cooperating with intelligence agencies, their work is by its very nature subject to fewer transparency requirements, safeguards and accountability measures than policing and law enforcement agencies, in particular in some of the less-than-democratic regimes that are of strategic interest to the EU. This raises significant reputational risks for Europol as an agency, and the EU as a whole. There is also a significant lack of transparency regarding Europol's current engagement with the intelligence agencies of third states, whether direct or indirect,[94] which should

93 Current priority states for signing cooperation agreements are Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey. See: Statewatch, 'Warnings over proposed new Europol partners in Middle East and North Africa', 14 May 2018, available at: https://www.statewatch.org/news/2018/may/eu-warnings-over-proposed-new-europol-partners-in-middle-east-and-north-africa/; Statewatch, 'Council bypasses Parliament onEuropol personal data exchange deals with Middle Eastern and NorthAfrican states', 18 June 2018, available at: https://www.statewatch.org/news/2018/june/eu-council-bypasses-parliament-on-europol-personal-data-exchange-deals-with-middle-eastern-and-north-african-states/

94 The states with which the agency has working arrangements are listed publicly on its website, but the agreements do not always list the specific authorities with which Europol cooperates. A notable case in point is the agreement with the United States of America, available here: https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1. It should also be noted that the existing "arrangement" for entering data received from third states in the SIS requires indirect cooperation between non-EU intelligence agencies and Europol, as the agency has a role in checking, validating and "enriching" lists of individuals initially sent to the member states. See: Matthias Monroy, 'German proposal: Prohibited EU secret service cooperation through the back door', 20 October 2020, https://digit.site36.net/2020/10/20/german-proposal-prohibited-eu-secret-service-cooperation-through-the-back-door/; Council of the European Union, 'Defining a process for evaluating and possibly entering information from third countries on suspected Foreign Terrorist Fighters in the Schengen Information System', document

be remedied.

While the EU's reputation for upholding fundamental rights may be called into question were cooperation with non-democratic regimes to be increased, the potential risks for individuals who may be subject to SIS alerts entered by Europol, based on data sourced from non-EU states, are much more serious. The persecution of dissidents through international policing databases is a well-established practice,[95] and while the proposals require that Europol carry out verifications of the information received from third countries prior to entering alerts in the SIS,[96] serious questions must be raised over its ability to undertake those verifications effectively, particularly given the limited requirements for those verifications set out in the proposal.

11564/3/20 REV 3, 16 November 2020, https://www.statewatch.org/statewatch-database/council-of-the-eu-defining-a-process-for-evaluating-and-possibly-entering-information-from-third-countries-on-suspected-foreign-terrorist-fighters-in-the-schengen-information-system/

95 See the heading 'International document databases as a tool of political persecution', https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/step-one-making-an-application/

96 Proposed Article 37a(3), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0791