8 July 2020

Feedback to the Roadmap to revise the mandate of the European Agency for Law Enforcement Cooperation (EUROPOL)

European Digital Rights (EDRi) is an association representing 44 human rights organisations from across Europe that defend rights and freedoms in the digital environment. This submission has been developed with the contributions from our members Statewatch (UK) and IT-Pol Denmark.

Summary

The Inception Impact Assessment[1] related to the Europol Regulation published on 14 May 2020 shares the European Commission's plans to further expand Europol's surveillance capacities by facilitating cross-border access to data for an agency whose mandate does not include law enforcement competences. In response to the Commission's consultation call, EDRi would like to share the following response:

- **EDRi recommends to first carry out a full evaluation of the 2016 Europol Regulation, before expanding the agency's powers, in order to base the revision of its mandate on proper evidence;**
- **EDRi opposes the Commission's proposal to expand Europol's powers in the field of data exchange with private parties as it goes beyond Europol's legal basis (Article 88(2));**
- **The extension of Europol's mandate to request personal data from private parties promotes the voluntary disclosure of personal data by online service providers which goes against the EU Charter of Fundamental Rights and national and European procedural safeguards;**
- **The procedure by which Europol accesses EU databases should be reviewed and include the involvement of an independent judicial authority;**
- **The Europol Regulation should grant the Joint Parliamentary Scrutiny Group with real oversight powers.**

Introduction

The planned legislative proposal follows a first revision of Europol's mandate that entered into force on 1 May 2017[2] and gave Europol a new authorisation to "receive" personal data, which is publicly available, from private parties like Facebook and Twitter directly.[3]

In 2020, the Commission and the Council want to extend Europol's powers again by allowing Europol to also *request* personal data directly from private parties. The Commission's Impact

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate
2 Regulation 2016/794 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
3 https://edri.org/europol-non-transparent-cooperation-with-it-companies/

Assessment concludes that the current situation limits "de facto (...) the Agency from cooperating effectively with entities like banks, online service providers and non-governmental organisations."

This potential expansion of Europol's mandate is part of a wider development in the field of European judicial and police cooperation. Several initiatives, like the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters (so called "e-evidence" Regulation), seek to enable law enforcement authorities to order the transfer of personal data directly from online service providers without the permission of the authorities of the Member States where the providers are established – and thus, bypassing the safeguards attached to the traditional judicial cooperation mechanisms.

Many critics, including EDRi[4], lawyers[5], academics[6], the European Data Protection Board (EDPB)[7], and other civil society organisations[8] oppose the very idea behind the e-evidence proposal because it is based on the false premise that criminal law is sufficiently harmonised in the EU and, as a result, heavily infringes fundamental rights without introducing the necessary safeguards. Eight EU Member States in the Council expressed doubts about the very constitutionality of this kind of proposal and criticised the "far reaching consequences (...) of the proposed regulation" as well as the lack of "checks and balances" and "guarantees for the protection of fundamental rights of citizens, freedom of press and freedom of expression and of public, national interests (...)". Finally, the previous European Parliament Committee responsible (Committee on Civil Liberties, Justice and Home Affairs, LIBE) expressed serious criticism in a series of Working Documents.[9]

EDRi opposes the Commission's proposal to expand Europol's powers in the field of data exchange with private parties for several reasons: (1) The lack of evidence and evaluation of the effectiveness of existing cross-border law enforcement instruments, (2) the original nature and mission of Europol as a European agency for law enforcement *cooperation* (among Member States), and (3) the poor level of meaningful human rights safeguards that would protect affected people from unwarranted data access. Specifically, the proposal to enable effective cooperation between Europol and private parities will **favour voluntary disclosure of personal data by private companies over compelled disclosure to Member States' law enforcement authorities in accordance with national or Union law**, which circumvents appropriate safeguards for fundamental rights (e.g. prior review by a court or an independent administrative authority).

1. The reform of the Europol Regulation should be based on evidence

In its Roadmap, the European Commission states that it does not intends to carry out an evaluation of Europol's current mandate because "the amount of evidence that can be collected for the

4 https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf
5 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf
6 https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/
7 https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_en
8 https://www.fairtrials.org/publication/cross-border-access-electronic-data
9 https://edri.org/libe-committee-analysis-challenges-of-cross-border-access-to-data/

purpose of a fully fledged evaluation is limited and non representative".

Although Regulation 2016/794 required the Commission to evaluate until 1 May 2019 in particular the practice of direct exchange of personal data with private parties, there is no public information on whether the Commission actually conducted such evaluation, what were its modalities as well as its results. **Without this evaluation, it is impossible to assess whether the current rules impede the fulfilment of the Agency's mission and whether the cooperation with private parties is indeed "insufficient".**[10]

Up until 2016, Europol's rules allowed the Agency to receive personal data from and share it with private parties only via national police units, assuming compliance with national laws. The new mandate adopted in 2016 enabled Europol to receive and share data itself provided the private party in question declares it is legally allowed to transfer that data and the transfer "concerns an individual and specific case", while "no fundamental rights [...] of the data subjects concerned override the public interest necessitating the transfer".[11] Paragraph 9 of Article 26, however, states that Europol must not contact private parties on its own initiative to retrieve or share personal data.

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[12] 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.**

The appetite to speed up procedures for cross-border access to data is equally surprising in the context of the "E-evidence" Regulation. Despite the recent adoption and early stages of implementation of the European Investigation Order (EIO), the Commission proposed a new legislative instrument. At the time of writing, however, **there has not been any assessment** of the use, efficiency and implementation of the EIO in terms of collecting electronic data[13], its impact on fundamental rights, and how the safeguards are being respected (or not) in practice. EDRi shared multiple times its concerns and stressed that the proposed E-evidence Regulation is premature, dangerous and lacks solid evidence.

2. Objective I. Enabling Europol to cooperate effectively with private parties

(a) Europol must not serve as a way around procedural safeguards and accountability mechanisms

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

10 https://www.statewatch.org/news/2019/aug/eu-council-europol-private-parties-10494-19.pdf
11 Article 26, Regulation 2016/794
12 https://data.consilium.europa.eu/doc/document/ST-14745-2019-INIT/en/pdf
13 https://www.europarl.europa.eu/doceo/document/E-8-2018-004970-ASW_EN.html

powers. It is only supposed to notify Member States of possible criminal offences in their jurisdiction, but 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 participating in joint investigation teams.

Unfortunately, Member States increasingly advocate to expand Europol's "operational" capacities and its power of own initiative. The main example of this development is the creation of the Europol Internet Referral Unit (IRU), which is tasked to monitor the internet and look for content that is likely "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 legitimate content. **This mechanism hardly complies with the EU Charter's** requirement that restrictions (on freedom of expression in this case) of fundamental rights must be "provided for by law" and not based on opaque "cooperation" between law enforcement authorities and private companies.

A similar conclusion can be drawn from the proposed policy options outlined in the Inception Impact Assessment, according to which Europol would be allowed to "process personal data (...) for purposes other than simply identifying the competent authority" and "to request data directly from private parties or query databases managed by private parties". **Such additional powers would be granted outside of the long-standing judicial cooperation framework and would completely fall short of the rights-protective procedural requirements and of strong judicial oversight** required under the rule of law (see (b) 2. below).

Furthermore, the **possibility for Europol to directly receive information by private parties is limited by its own legal basis.** Indeed, **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). This can **hardly encompass Europol receiving and actively requesting data from private companies on a larger scale.**

(b) Cooperation with private parties cannot happen at the detriment of fundamental rights and the rule of law

1. The principle of territoriality should be respected

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 cannot effectively fulfil its responsibility to protect the fundamental rights of its citizens since it has no knowledge of

14 https://edri.org/context-in-terrorist-content-online/

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, **Europol should not be allowed to request and process personal data without the authorisation of the executing authority.**

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.[15]

2. No access should be granted without prior judicial authorisation

Considering the functions granted to Europol by the Treaties, the Agency cannot possibly meet the criteria of a competent authority under EU law. Judicial review and validation by such a competent authority are, however, 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.[16] 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 jurisprudence.[17] **Europol does not fall within the definition of a court or an independent administrative authority to access personal data as required by the CJEU.**

Moreover, since Europol is not a competent authority with executive powers, the proposal for effective cooperation with private parties would institutionalise a system of voluntary disclosure of personal data by online service providers and other private companies. EDRi has consistently opposed voluntary disclosures of personal data[18] 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

15 https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf

16 Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Ireland, 8 April 2014.

17 In the Tele2/Watson case the CJEU ruled that "it is essential that access of the competent national authorities to retained data should, as a general rule, be subject to a prior review carried out by a court or independent administrative body, except in cases of validly established urgency." Joined Cases C-203/15 and C-698/15 Tele2 Sverige and Tom Watson, Judgment of 21 December 2016, http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

18 See e.g. EDRi submission to the Council of Europe on Second Additional Protocol to the Budapest Convention on Cybercrime https://edri.org/files/consultations/globalcoalition-civilsocietyresponse_coe-t-cy_20180628.pdf and https://edri.org/wp-content/uploads/2019/11/20191107_CivilSocietySubmission_TCYDraftSecondAdditionalProtocol.pdf

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 enforcement 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.

3. Objective III. Streamlining Europol cooperation with third countries: exchanges with third countries should take place in the current data protection framework

After the entry into force of the General Data Protection Regulation[19] and the Police Directive[20], it is crucial that **transfers to third countries and international organisations can only take place on the basis of adequacy or a binding agreement providing adequate safeguards.** A binding agreement will ensure legal certainty as well as full accountability of Europol for the transfer and should always be requirement for massive, structural and repetitive transfer of personal data. In any event of a data transfer, appropriate safeguards should exist to ensure that individuals' rights are enforceable and effective legal remedies are available following the transfer.

According to Europol's programming document 2020-2022[21], priority agreements on the transfer of personal data between Europol and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey are currently negotiated. All these countries have very poor records in terms of democratic standards, the rule of law and the respect of human rights, especially human rights abuses committed by law enforcement authorities. Up to now, many of them do not have any legally binding data protection instrument in place. In addition to loosening Europol's conditions for transferring data to third countries, these agreements risk undermining the quality of the protection of the personal data of European data subjects.

Lastly, the idea outlined in Option 3 of this policy objective according to which Europol would be competent to assess by itself that the level of protection of personal data in a third country is adequate in order to permit transfers is incompatible with current law. This task should remain within the remit of the Commission's and the European Data Protection Supervisor's mandates.

4. Additional comments

(a) Access to EURODAC and VIS systems should be submitted to a data protection review

Europol has access to the Visa Information System (VIS) and European Dactyloscopy (Eurodac)

19 (EU) 2016/679
20 (EU) 2016/680
21 https://www.europol.europa.eu/publications-documents/europol-programming-document

databases which contain personal data of asylum applicants and migrants (including biometric data). However, the current procedure by which the Europol has access remains problematic as regards the requirement for national and European access points to act independently. In the case of Europol, the Agency effectively authorises itself, because it nominates an access point within one of its own internal departments, that is responsible for assessing requests from other Europol officials.

Such procedure is described in Article 7 of the Eurodac Regulation[22] for example: "Europol shall designate a specialised unit with duly empowered Europol officials to act as *its verifying authority, which shall act independently of the designated authority* referred to in paragraph 2 of this Article when performing its tasks under this Regulation and *shall not receive instructions from the designated authority as regards the outcome of the verification.* The unit shall ensure that the conditions for requesting comparisons of fingerprints with Eurodac data are fulfilled." (emphasis added).[23]

It is questionable that this can really amount to an "independent" verification. Furthermore, this procedure has never been examined and confirmed that it fulfills the independency requirements. **In the framework of the Europol Regulation revision, EDRi therefore recommends that a data protection review is carried out to determine how the procedure works in practice, and that access to EU databases is made conditional to the authorisation of genuinely independent and judicial authorities (see 2.(b)2. above).**

(b) Oversight mechanisms should be strengthened

The envisaged updates to the Europol Regulation would create far-reaching new data-processing capabilities for Europol. Yet there is no indication in the Commission's roadmap that the current oversight mechanisms will be revised and adapted to this expanding mandate.

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. EDRi already voiced its strong concerns with regards to the applicability of the current mechanism.[24] 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. The idea is merely to "politically monitor Europol's activities". Europol is rarely faced with any significant scrutiny of the administration and organisation of its work, in particular its operational work.

The European Commission should ensure that:

- **An evaluation of the work of the JPSG is part of the Europol Regulation fully-fledged evaluation in order to determine whether or not it has been able to carry out its missions;**
- **The future Europol regulation provides the JPSG with real powers of supervision by:**

22 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0603&from=EN
23 For the VIS database, see Article 7, Council Decision 2008/633/JHA, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008D0633
24 https://edri.org/oversight-new-europol-regulation-likely-remain-superficial/

- **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**

In addition, the European Commission should consider opening a debate on 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" -- which has been involved in data scandals and criticised for its close ties to far-right politicans across the globe -- was only made public and known to MEPs recently.[25] 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**.

5. Conclusion

The example of the Europol IRU shows that Member States are keen on setting up new operational duties that are non-transparent and are not subject to neither parliamentary scrutiny nor judicial oversight. This policy agenda is at odds with transparency requirements that ensure that Europol remains a fully accountable organisation.

25 https://www.europarl.europa.eu/doceo/document/E-9-2020-000173-ASW_EN.html