CM2114

COMMENT ON PROPOSED EXTENSIVE DATA PROCESSING POWERS FOR EUROPOL

October 2021

In December 2020, the European Commission issued a Proposal to amend the Europol Regulation regarding 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. This amendment considerably expands the data processing powers of Europol without establishing an independent oversight over Europol's dat processing power. This could possibly have adverse effects on the fundamental rights of affected persons, both suspects and innocent people.

Meijers Committee

Standing committee of experts on international immigration, refugee and criminal law

Introduction

In December 2020, the European Commission issued a Proposal to amend the Europol Regulation regarding 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. In October 2021, the LIBE Committee of the European Parliament has voted in favour of the proposal. Now, the Commission, the Council and the Parliament must negotiate the final version of the bill.

This amendment considerably expands the data processing powers of Europol and could possibly have adverse effects on the fundamental rights of affected persons, both suspects and innocent people. With regard to this proposal and the extensive powers without independent oversight that Europol gains, the Meijers Committee wishes to make the following observations and recommendations.[1]

Data processing powers

Parts of the proposed amendments aim to legalise personal data processing activities that Europol is already conducting, such as the processing of large datasets and the processing of data about individuals not linked to any criminal activity. In September 2020, the EDPS admonished Europol for these (currently) unlawful data processing activities and urged Europol to mitigate the risks created by these data processing activities. The Commission responded to the EDPS's statement by proposing certain amendments to the Europol Regulation to create a legal basis for Europol's extensive data processing activities.

Tension between Europol's supportive and proactive role

The proposed amendments to the Europol Regulation foresee a proactive role for Europol. Europol will receive a new task: "proactively monitor and contribute to research and innovation activities" (Article 4(1)(t) as proposed). Furthermore, Europol will be empowered to receive personal data directly from private parties and then forward the personal data to the national units concerned (Article 26(2) as proposed). In connection to that, Europol may transmit or transfer personal data to private parties in specific cases (Article 26(5) as proposed), and Europol may request Member States, via their national units, to obtain personal data from private parties (Article 26(6a) as proposed).

As Vavoula and Mitsilegas remark in their study for the European Parliament, "[m]agnifying Europol's role towards the direction of proactivity somewhat sits at odds with Article 88(1) TFEU, according to which Europol has a supportive role and its tasks are heavily relied on Member States' willingness to cooperate".

The use of personal data for validation of algorithms should be strictly necessary

Europol's new task to proactively monitor and contribute to research and innovation activities includes "the development, training, testing and validation of algorithms for the development of tools" (Article 4(1)(t) as proposed). In addition to that, Europol is empowered to process personal data for research and innovation activities (Article 18(5)(e) as proposed).

[1] Some comments in this note have already been published in a blogpost by Sarah Eskens on European Law Blog: https://europeanlawblog.eu/2021/07/30/new-and-extensive-data-processing-powers-proposed-for-europol/

In Opinion 1/15 on the Draft agreement between Canada and the EU on the transfer and processing of PNR data, the CJEU held that the "systematic use of PNR data for the purpose of verifying the reliability and topicality of the pre-established models and criteria on which the automated processing of that data is based (...) or of defining new models and criteria for such processing" must be strictly necessary.

The proposed amendments do not contain a strict necessity test for the validation of algorithms. The proposed amendments state that research and innovation projects should have "clearly defined objectives, duration, and scope of the personal data processing involved" (Article 18(3a) as proposed). A new Article 33a (as proposed) contains further rules for the processing of personal data for research and innovation, albeit without a condition of strict necessity of the data processing. The Meijers Committee recommends including such a condition of strict necessity.

Technological reality becomes normative reality

The Explanatory Memorandum states that Europol needs new data processing powers because it is receiving larger and more complex datasets from Member States. This shows that the Commission takes it as a given that national authorities have large and complex datasets and that they submit these to Europol. However, this line of thought uncritically accepts that a technological reality (there are large datasets) becomes a normative reality (Europol should be able to process these datasets).

It is expected that a similar logic will be followed regarding Europol's research and innovation activities. The proposed amendments empower Europol to monitor and contribute to research and innovation activities, "including the development, training, testing and validation of algorithms" (Article 4(1)(t) as proposed). Once Europol develops new and powerful algorithms that can be used to analyse large datasets, the argument will be made that Europol or national authorities should be able to use these algorithms simply because they are available.

Open norms for analysis of personal data outside Annex II

The large and complex datasets that Europol regularly receives contain both personal data that Europol is allowed to process and personal data that Europol may not process. The Europol Regulation provides that for the purpose of crosschecking, strategic or operational analysis, information exchange, or (new!) research and innovation, Europol may collect and process personal data related to only certain categories of data subjects (Article 18(5)). Annex II to the Europol Regulation lists those categories, which include persons suspected of having committed a criminal offence and persons being a contact or associate of suspected persons.

As noted above, Europol is currently already unlawfully processing data about individuals who are not linked to any criminal activity for crosschecking, strategic or operational analysis, or information exchange. The Commission aims to legalise this practice by empowering Europol to temporarily process personal data for determining whether such data are listed in Annex II of the Europol Regulation and may be processed for the purposes mentioned above (Article 18(5a) as proposed). This "pre-analysis" of data includes checking the data against all data that Europol already processes in accordance with the law (Article 18(5a) as proposed).

In connection to that, the proposed amendments introduce a new Article 18a which empowers Europol to process personal data outside the categories of data subjects listed in Annex II, where necessary for the support of a specific criminal investigation (Article 18a(1) as proposed).

The pre-analysis of data and the processing of data in support of a specific criminal investigation are regulated by open norms that are difficult to oversee or supervise by external bodies such as the European Parliament or EDPS. For both data processing activities, the Management Board of Europol will further specify the conditions relating to the processing of such data (Article 18(5a) and Article 18a(2) as proposed). In other words, when Europol processes large sets of personal data for which it is unclear whether Europol is actually allowed to process these data and which most likely contain data of people who are not linked in any capacity to a crime, then Europol themselves can determine the rules for such data processing. The proposed amendments require that in both cases, Europol consults the EDPS. However, it will be difficult for the EDPS or any other external body such as the European Parliament to evaluate the conditions that the Management Board specifies if the new Europol Regulation does not contain any criteria for these further conditions.

Specific criteria are also missing for the duration of the pre-analysis of data. The proposed amendments state that Europol may conduct a pre-analysis of data for a maximum period of one year, or in "justified cases" for a longer period with the prior authorisation of the EDPS (Article 18(5a) as proposed). The proposal does not indicate what justified cases are and how the EDPS should assess whether longer processing is justified. In its Opinion on the proposed amendments, the EDPS warns that "[g]iven the lack of specific criteria or at least general indication what should be considered as 'justified cases', the prior authorisation of the prolongation by the EDPS could actually turn into 'rubber-stamping' of the requests by the Agency".

New data processing powers should not become the rule

The two new data processing powers described in the previous section, namely pre-analysis of data (Article 18(5a)) and the processing of data in support of a criminal investigation (Article 18a), involve the processing of personal data outside the categories of personal data and data subjects listed in Annex II of the Europol Regulation. This means that these new data processing powers form an exception to the rule that Europol may collect and process only categories of personal data and data subjects explicitly and exhaustively listed in Annex II (Article 18(5)).

There need to be sufficient safeguards for both new data processing powers to ensure that the exception does not become the rule. The EDPS, therefore, proposes in its Opinion on the proposed amendments that the pre-analysis of data should be limited to cases where such pre-analysis is an "objective necessity". Similarly, the EDPS recommends the introduction of more safeguards in Article 18a to prevent that this derogation does not become the rule. To that end, the EDPS recommends that the amended Regulation "should lay down certain conditions and/or thresholds, such as scale, complexity, type or importance of the investigations" for which data outside of Annex II may be processed.

Voluntary data transfer by private parties circumvents procedural requirements

Article 26(2) as proposed enables Europol to receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned. This sets up a system that relies on and incentivises voluntary data sharing by private parties to Europol. Currently, Europol can process personal data received from private parties in three specific and limited cases. A Study on the practice of direct exchanges of personal data between Europol and private parties, conducted by Milieu Consulting for the European Commission, identified several limitations to the system of personal data exchange between private parties and Europol. It also observed an increasing

willingness of online service providers to take the initiative to share personal data with Europol outside of the regulated system.

To resolve these difficulties and capitalise on private parties' willingness to share data, the Commission proposes to establish Europol as a single point of contact for private parties. Recital 26 of the proposal notes that "[a]s a result from the increased use of online services by criminals, private parties hold increasing amounts of personal data that may be relevant for criminal investigations". The Commission wants to incentivise the disclosure of data by making it easier for private parties to share such data directly with Europol voluntarily.

As EDRI has pointed out in its Recommendations on the revision of Europol's mandate, a system of voluntary data transfer by private parties to Europol "takes place without the procedural safeguards which apply to [national] 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". In most data transfers from private parties to Europol, the transfer generally happens because private parties receive a request from the national law enforcement authority in the context of criminal investigations or because private parties are under a legal obligation to report data to the national law enforcement authority. Information gathered by the national police and forwarded to Europol is also generally related to suspected criminal offences or is related to certain persons suspected of having committed a criminal offence. These routes are regulated by procedural requirements such as judicial authorisation of an information request or strict legal requirements regarding the forwarding of data via the intermediaries to Europol. When Europol is empowered to process personal data directly received from private parties, these procedural and other legal requirements that protect individual rights are circumvented. Information received from private parties is combined with other information, analysed, and probably sent forward to member states interested in the information. The proposal also enables Europol to request a member state to start an investigation if there is a basis for that in the information that it received. There are many questions relating to the status of the gathered information and whether it leads to admissible evidence in court.

Transfer of personal data by Europol to private parties

The proposal is that Europol may transmit or transfer personal data to private parties (Article 26a sub 3) under certain circumstances. Within Europol, who will decide on this? In addition, who will supervise this activity? In the national system, the Public Prosecutor's office oversees the criminal investigation, and when the police use special powers, permission is first required from the public prosecutor. The regulation does not contain a procedure requiring a decision by a public prosecutor or an investigating judge prior to Europol transmitting this information.

Furthermore, there are no safeguards limiting private parties in processing the information that Europol shared. For example, are private parties allowed to disclose that information to other parties? Unlike Europol, states have the possibility to impose restrictions or conditions on private parties and have the possibility to sanction private parties when these restrictions or conditions are violated. Therefore, the Meijers Committee recommends leaving it to the national states to gather information with private parties, after which this information can be shared with Europol. Based on the proposed Article 6a, Europol can request the member states to obtain personal information from private parties. When the information has been collected in accordance with national law, there can be no discussion about the legal status of this information. The Meijers Committee also recommends leaving it to national authorities to share information with private parties. In this way, there is a built-in supervision, and national authorities can monitor the way the information is dealt with.

Exchange between Europol and the European Public Prosecutor's Office

In its proposal, the Commission also includes provisions for the exchange of information between Europol and the European Public Prosecutor's Office (EPPO) (Articles 18a, 20a and recital 22). These provisions are intended to strengthen the cooperation between Europol and EPPO. In the proposal as amended by the Council, the Council inserted an extra recital 17a that is relevant for the relationship between Europol and the EPPO. This recital states that Europol should be able to use investigative data processed by EPPO and submitted by EPPO 'within its competences to Europol for support'. This language is a bit ambiguous in that it could be read as referring to support given by Europol to the EPPO or the other way around. The only possible interpretation would be that it refers to the EPPO seeking the support from Europol in a specific investigation as mentioned in Article 102(2) of Regulation 2017/1939 establishing the EPPO (The EPPO Regulation). Importantly, the EPPO Regulation clearly refers to analytical support in the context of a specific investigation. The recital could be read as suggesting a wider selection of investigative data that could be sent from EPPO to Europol. More specifically, Article 99 and 100 of the EPPO Regulation, laying down common provisions on relations of the EPPO to other Union institutions, restrict the transfer of information from the EPPO to these other bodies to exchanges that are relevant and/or necessary for the performance of the tasks of the EPPO. Consequently, the EPPO is not competent to transfer to Europol information of an investigative or other nature in cases where such might be in the interest of Europol's duties but not necessary or relevant for the performance of the EPPO's duties. Recital 17a should therefore make clear that the 'support' intended there is the support that Europol can offer the EPPO and not the other way around.

The Commission proposes in Article 20a(4) to oblige Europol to report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence. This provision is largely a repetition of the already existing obligation for Europol to report these offences, laid down in Article 24(1) of Regulation 2017/1939. A repetition as such might not do much harm, but there is a risk that some elements of the duty to report are left out. That is, for instance, the case with the duty laid down in Article 14(5) of Regulation 2017/1939 to report cases that could potentially fall under the EPPO's competence, but for which an assessment whether they fulfil the criteria of Article 25(2) are met is not possible. Leaving out this duty to report could lead to under-reporting from Europol to EPPO. For that reason, it would be better to either fully include all Europol's reporting duties in the Europol Regulation or leave them out for the reason that they are already included in the EPPO Regulation.

Article 18a(1a) lays down duties for Member States and the EPPO for cases in which these authorities have provided Europol with investigative data, and the mandate to process these data has ceased to exist. In such cases, these authorities are obliged to inform Europol of their lack of mandate to process the data. However, the proposal does not make clear what the consequence of that notification is. Should Europol, upon receiving such a notification, stop processing the investigative data altogether, or may it continue doing that as the lack of mandate on the side of the Member State or the EPPO does not impact Europol's competence to process this data? The Meijers Committee recommends clarifying the Regulation in such a way that it is clear that Europol is no longer competent to process investigative data that it has received from a Member State or the EPPO in case it is informed that the Member State or the EPPO does not have any competence any more to process the data.

Recommendations

- Include a strict necessity test for the processing of personal data for research and innovation.
- Critically assess the fact that technological reality (there are large datasets) becomes a normative reality (Europol should be able to process these datasets).
- The pre-analysis of data as well as duration of this analysis about individuals who are not linked to any criminal activity for crosschecking, strategic or operational analysis or information exchange should include specific criteria.
- New data processing powers should not become the rule: clear and sufficient safeguards need to be implemented.
- Ensure that procedural and other legal requirements that protect individual rights are not circumvented when Europol receives personal data directly from private parties.
- Include a procedure requiring a decision by a public prosecutor or an investigating judge prior to Europol transmitting personal data to private parties and leave it to national authorities to gather information with private parties, after which this information can be shared with Europol, and to share this information with private parties.
- Clarify Europol's relation to EPPO by either fully including all Europol's reporting duties in the Europol Regulation or leaving them out because they are already included in the EPPO Regulation.

About

The Meijers Committee is an independent group of experts that researches and advises on European criminal, migration, refugee, privacy, non-discrimination and constitutional law.


post@commissie-meijers.nl


+ 31 20 362 05 05


commissie-meijers.nl


Twitter


LinkedIn