Article 29 (6a)

Without prejudice to Directive (EU) 2016/680, in the framework of an investigation for the targeted search of a person convicted or suspected of having committed a criminal offence, the deployer of an AI system for post-remote biometric identification shall request an authori~~s~~zation, ***prior, or*** ~~***in exceptional cases,***~~ without undue delay ***and no later than*** ~~***24/***~~***48hours***, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of the system, except when the system is used for the initial identification of a potential ***suspect***~~***ed***~~ ~~**offender**~~ ***based on objective and verifiable facts directly linked to the offence***. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence.

If the requested authori~~s~~zation provided for in the first subparagraph of this paragraph is rejected, the use of the post remote biometric identification system linked to that authori~~s~~zation shall be stopped with immediate effect ***and the personal data*** *linked to the use of the system for which the authorisation was requested* ***shall be deleted.***

In any case, such AI system for post remote biometric identification shall not be used for law enforcement purposes in an untargeted way, without any link to a criminal offence, a criminal proceeding, ~~**or the prevention of**~~ a ***genuine and present*** *or genuine and foreseeable* ***threat of a criminal offence*** ~~**criminal offence**~~ or the search for ***a*** specific missing person~~**s**~~.

It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities solely based on the output of these post remote biometric identification systems.

This paragraph is without prejudice to the provisions of Article 10 of the Directive (EU) 2016/680 and Article 9 of the GDPR for the processing of biometric data. ~~**for purposes other than law enforcement**~~.

Regardless of the purpose or deployer, each use of these systems shall be ~~**entered**~~ documented in the relevant police file and shall be made available to the relevant market surveillance authority and the national data protection authority upon request, excluding the disclosure of sensitive operational data.

~~**After putting into service *Deployers of* post remote biometric systems, deployers shall *log and notify each use to the relevant market surveillance and national data protection authorities.***~~

~~***The notification can be submitted as an aggregation of uses over the course of no longer than 30 days.***~~ ***Deployers shall, in addition,*** submit annual reports to the relevant market surveillance and national data protection authorities on the ~~[aggregated]~~ uses of post-remote biometric identification systems, excluding the disclosure of sensitive operational data related to law enforcement. ***The reports can be aggregated to cover several deployments in one operation.***

Member States may introduce, in accordance with Union law, more restrictive laws on the use of post remote biometric identification systems.

Recitals:

(XX) Each supervisory authority [under Art. 63(5)] should have effective investigative and corrective powers, including at least the power to obtain access to all personal data that are being processed and to all information necessary for the performance of its tasks. The supervisory authorities should be able to exercise their powers by acting with complete independence. Any limitations of their access to sensitive operational data under this Regulation should be without prejudice to the powers conferred to them by Directive 2016/680.

(XY) Any processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU) 2016/680, that allows such processing only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and where authorised by Union or Member State law. Such use, when authorized, also needs to respect the principles laid down in Article 4 paragraph 1 of Directive (EU) 2016/680 including lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation

(YY) Without prejudice to applicable Union law, notably the GDPR and Directive (EU) 2016/680 (the Law Enforcement Directive), considering the intrusive nature of post remote biometric identification systems, the use of post remote biometric identification systems shall be subject to safeguards. Post biometric identification systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed dataset of legally acquired video footage. In any case, post remote biometric identification systems should not be used in the framework of law enforcement to amount to indiscriminate surveillance. The conditions for post remote biometric identification should in any case not provide a basis to circumvent the conditions of the prohibition and strict exceptions for real time remote biometric identification.