European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 159-165
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 14

*The Conseil d'Etat Finds the Use of Facial Recognition by Law Enforcement Agencies to Support Criminal Investigations "Strictly Necessary" and Proportional**

Theodore Christakis
(Professor of International and European law – Université Grenoble Alpes & Director of the Chair on the Legal and Regulatory implications of AI)

Alexandre Lodie
(Doctor of International Law – Université Grenoble Alpes & Research Fellow – Chair on the Legal and Regulatory implications of AI)

French Council of State, *Decision n. 442364, 26 April 2022*

The Conseil d'État dismissed a legal challenge initiated by the French NGO "La Quadrature du Net" which claimed that the use of facial recognition by law enforcement agencies in criminal investigations to help identify suspects who appear in the TAJ System ("Traitement des antécédents judiciaires" - Criminal Case History Database) did not meet the EU Law Enforcement Directive's "absolute necessity" and proportionality requirements. In this case the French NGO "La Quadrature du Net" (LQDN) asked the French Supreme Administrative Court to invalidate article R 40-26 of the code of criminal procedure which expressly provides for the use of facial recognition to aid in the identification of suspects during criminal investigations. LQDN considered that the use of this technology was not "absolutely necessary" as required by the French version of Article 10 of the Law Enforcement Directive (LED). The Court dismissed this claim considering that given the vast amount of data contained in the TAJ database, the automated data processing was absolutely necessary. This decision feeds into the debate about how to interpret the strict necessity requirement laid down by the LED concerning the use of facial recognition.

ABSTRACT In this case the French supreme Administrative Court (Conseil d'Etat) was seized by a French NGO called 'La Quadrature du Net'. The NGO asked the Court to overturn the French Prime Minister's implicit decision to refuse to repeal some provisions of Article R 40-26 of the French Code of Criminal Procedures which enable the use of Facial Recognition by Law enforcement authorities to support criminal investigations. The Court dismissed this claim, arguing that these provisions are strictly necessary and proportionate to the aim pursued and thus compliant with the law enforcement directive.

1. *Setting the scene*

The use of facial recognition for crime prevention, investigation and repression has been under the spotlight for many years in France. In particular, the French NGO LQDN, which is a privacy and a numerical rights advocate, has repeatedly spoken out against the deployment of what it considers an intrusive technology.[1] One of the main targets of the LQDN's criticism has been the "Traitement des antécédents judiciaires" (TAJ), which is a police criminal case history database provided for by a 2012 decree,[2] which became operational in 2013. A new article was inserted into the code of criminal

* Article submitted to double-blind peer review.

[1] Facial recognition of demonstrators is already authorised, in *La Quadrature du Net*, 18 November 2019, available at: www.laquadrature.net.

[2] See Decree 4 May 2012, No. 652 concerning the processing of criminal record, available at: www.legifrance.gouv.fr/loda/id/JORFTEXT000025803463.

procedure as a result of this decree, which expressly provides law enforcement authorities with the option of retaining photographs of suspects or criminals for face matching at a later date via facial recognition software.[3] In other words, the system allows for the probe image of a suspect (from video surveillance footage or photographs) to be compared with images stored in the TAJ database (1-M).

As indicated in the TELEFI Report of October 2019, "the number of facial images on the TAJ was approximately 6 million out of which more than 99% were controlled images of suspects and victims (i.e. unknown dead bodies, the seriously injured and missing persons) whilst the rest (approximately 6000) were uncontrolled images (e.g. photo robot sketches, surveillance images etc.)".[4] The TAJ is populated with images that are captured and registered by the two police organisations in France, the National Gendarmerie and the National Police. Facial recognition is solely used as an investigative tool by investigators who perform searches. The law enforcement agencies and the Ministries of the Interior and Justice in France insist that such search results are used for operational purposes to support investigations, and not as evidence in court. The search results return a list of candidates, which is manually evaluated by the investigator conducting the search in order to decide whether the list contains a candidate likely to have been involved in a particular crime.

According to the TELEFI Report, "in 2018, approximately 200 000 searches were performed and a further 250 000 took place during the first eight months of 2019".[5] This system enabled, for instance, the identification, arrest and resulting conviction by the Lyon criminal Court of a man who stole a truckful of goods in a warehouse in the Lyon suburbs.[6] This case raised a lot of interesting issues. The defendant's attorney claimed that his client was used as a "guinea pig" for facial recognition[7] and he unsuccessfully challenged the use of the technology which helped identify his client. Indeed, in this case the Lyon criminal Court accepted the arguments of the prosecutor and the law enforcement authorities, that facial recognition was solely used to support the investigation and did not constitute "evidence" as such.

In 2012 already, the French branch of the NGO, the "Ligue des droits de l'Homme" was one of the first to challenge, before the Conseil d'Etat, the lawfulness of the decree authorising the use of facial recognition in relation to the TAJ system. The highest French administrative Court then confirmed the lawfulness and validity of the 2012 decree authorising the TAJ. It concluded that "The procedures for collecting, consulting and processing such data, under the conditions defined by the contested decree, are such as to guarantee the effectiveness of the establishment of offences that are against the criminal law, the gathering of evidence of such offences and the search for their perpetrators; that it follows that the collection of digitised photographs of persons implicated or under investigation or inquiry for the search for the causes of death or disappearance is, taking into account the restrictions and precautions to which this processing is subject, adequate, relevant and not excessive in relation to the legitimate purposes".[8]

Despite this initial ruling which validated the decree introducing the TAJ, La Quadrature du Net filed a new complaint in 2020

[3] In particular, article R 40-26 of the code of criminal procedure reads as follows: "The following categories of personal data and information may be recorded in this processing operation 1° Concerning the accused persons : a) Natural persons: […] - a photograph with technical features that allows a facial recognition device to be applied to it (facial photograph) […] 3° Concerning persons who are the subject of an investigation or enquiry into the causes of death or disappearance: […] - Photographs with technical characteristics that allow a facial recognition device to be applied to it (facial photographs of missing persons and unidentified bodies".

[4] *Summary report of the project 'Towards the European Level Exchange of Facial Images*, *Telefi Project*, Version 1.0, January 2021, 70, available at: https://www.telefi-project.eu/sites/default/files/TELEFI SummaryReport.pdf.

[5] *Ibidem*, 72.

[6] R. Gardette, *Un logiciel de reconnaissance faciale utilisé lors d'un procès à Lyon fait débat*, France 3 régions, 18 September 2019, available at: https://france3-regions.francetvinfo.fr/auvergne-rhone-alpes/rhone/lyon/logiciel-reconnaissance-faciale-utilise-lors-proces-lyon-1724157.html.

[7] D. Lepetitgaland, *Première en France: à Lyon, la reconnaissance faciale le désigne, il est condamné*, *Le Progrès*, 1 November 2019, available at: www.leprogres.fr/rhone-69/2019/11/01/la-reconnaissance-faciale-le-designe-il-est-condamne.

[8] Conseil d'État, 10ème / 9ème SSR, 11 April 2014, 360759, available at: www.legifrance.gouv.fr/ceta/id/CETATEXT000028842861.

requesting that the Conseil d'État invalidate the provisions in the code of Criminal Procedure which expressly concern the option of resorting to facial recognition technology in combination with the TAJ database. LQDN's request therefore specifically concerned the use of facial recognition and not the TAJ system as a whole. It was also unprecedented in that it was based on the claim that the relevant provisions of the French code of Criminal Procedure were contrary to Article 10 of the LED, which was adopted in 2016 and only entered into force in 2018. This complaint led to the decision issued on 26 April 2022 by the Conseil d'Etat.

2. *The LQDN's claims*

As mentioned above, LQDN is a fierce opponent of facial recognition technology. On 12 November 2019 LQDN issued "a request for the repeal of paragraphs 16 and 59 of Article R. 40-26 of the Code of Criminal Procedure, which describes the TAJ system" to the Prime Minister, Minister of the Interior and the Minister of Justice.[9]

Since the Government did not repeal the contested provisions, LQDN referred their tacit refusal to invalidate the provisions to the Conseil d'Etat. LQDN challenged the idea that article R 40-26 of the code of criminal procedure complies with article 10 of the Law enforcement directive, which provides that "[p]rocessing of […] biometric data for the purpose of uniquely identifying a natural person […] shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject".[10]

It is important to note from the outset that that the French version of the LED translates the "strict necessity" criterion as "necessité absolue", which translates back as "*absolute* necessity". This translation seems to increase the significance of the necessity criterion.

LQDN claimed that "there is no 'absolute necessity' that can legally justify such measures in this case".[11] In its letter of response to LQDN sent on February 12 , 2020, the Minister of Justice stated that "the facial recognition device constitutes a technical aid to the investigator's reconciliation of information obtained in the course of the investigations carried out".[12] LQDN seems to consider that since the Government describes facial recognition as a mere "technical aid" to police officers, this tool is not "absolutely necessary" to carry out the investigation and the image matching used to identify suspects. On this topic LQDN stated that "[t]he role of 'technical assistance', is in essence not in accordance with the 'absolute necessity' criterion. In other words, recognising the mere 'usefulness' of the device demonstrates the absence of 'necessity' and, a fortiori, the absence of the 'absolute necessity' required to legally justify such a device".[13] LQDN therefore considered that something which is merely viewed as a form of assistance cannot at the same time be viewed as indispensable. However, the Conseil d'Etat did not agree.

3. *The Conseil d'Etat's interpretation of the strict necessity requirement*

Even though the French version of Article 10 of the LED seems to propose an interpretation of the "strict necessity" requirement that is even more rigid than that used in the English version, the Conseil d'Etat did not accept the LQDN interpretation. On the contrary, it concluded that: "[i]n view of the number of defendants registered in this processing, which amounts to several million, it is materially impossible for the competent officers to carry out such a comparison manually, and moreover with the same degree of reliability as that offered by a correctly parameterised facial recognition algorithm. However, such an identification based on a person's face and the comparison with the data recorded in the [TAJ] may prove to be absolutely necessary for the search for the perpetrators of offences and for the prevention

[9] See Conseil d'Etat, Section du contentieux, requête, 2 August 2020, available at: www.laquadrature.net/wp-content/uploads/sites/8/2020/08/LQDN-REQ-TAJ-02082020.pdf.

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[11] See Conseil d'Etat, Section du contentieux, requête, 2 August 2020, 6., available at: www.laquadrature.net/wp-content/uploads/sites/8/2020/08/LQDN-REQ-TAJ-02082020.pdf.

[12] *Ibidem*.

[13] *Ibidem*.

of breaches of public order, both of which are necessary to safeguard rights and principles of constitutional value. Consequently, the recording of the data at issue in this processing operation meets the condition of absolute necessity laid down by the above-mentioned provisions".[14]

In other words, as regards the vast number of individuals included in the TAJ system, the facial recognition software is absolutely necessary for police officers to be able to effectively compare images in order to identify suspects and support criminal investigations.

This rationale did not convince LQDN, which characterised the Conseil d'Etat's reasoning as "circular".[15] LQDN questioned use of the TAJ precisely because it considered this database to be "a mass surveillance tool", which is so massive that it necessitates the use of facial recognition in order for it to work. Therefore, according to LQDN, the Conseil d'Etat reinforces the logic of surveillance more than it diminishes it. LQDN stated to prove this point that "[o]ne mass surveillance (generalised data collection) requires another mass surveillance (generalised facial recognition)".[16]

However, the Conseil d'Etat's reasoning is not really surprising since it had already had the opportunity to interpret the strict (or "absolute" in French) necessity requirement in relation to article 88 of the amended law of 6 January 1978 - which basically transposes article 10 of the LED into French law - in a decision dated 4 January 2021.[17] The Conseil d'Etat had to rule on the lawfulness of a decree which modified certain provisions related to the "Prévention des atteintes à la sécurité publique" ("prevention of public security breaches") database, which is another police database.[18] The abovementioned decree empowered the police to collect and store data containing people's political opinions, religious beliefs, and many other sensitive data, for specific purposes such as the protection of State security.[19] On that occasion, the Conseil d'Etat stated the following: "Article R. 236-12 of the Internal Security Code, as drafted by Article 2 of the contested decree, provides that data may only be recorded insofar as they are strictly necessary for the purposes of the processing. It specifies that only activities 'likely to undermine public security or State security' may give rise to the recording of data on public activities or activities within groups or legal entities or activities on social networks, which prohibits, in particular, the recording of persons in the processing operation based on mere trade union membership. It should also be noted, as the administration argued before the interim relief judge, that the possibility of recording data relating to activities likely to undermine public security on the networks can only come from data collected individually and manually. […] In these circumstances, it does not appear, in the light of the investigation, that the processing of these data does not meet an absolute necessity with regard to the purposes of preventing risks to public security and is not accompanied by appropriate guarantees".[20]

In conclusion, the Conseil d'Etat considered that the processing of sensitive data was compliant with the 'absolute necessity' requirement as laid down by article 88 of the law of 6 January 1978 be it for protecting State security or to carry out investigations. It remains to be seen whether the Conseil d'Etat would have been able to criticise article R 40-26 of the code of criminal procedure on other grounds, such as the proportionality requirement.

4. *Ex-post biometric identification and the proportionality requirement*

The proportionality principle complements the necessity principle, since for a data processing operation to be deemed lawful, it must be strictly necessary and proportionate to

[14] Conseil d'État, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.
[15] *Le Conseil d'Etat sauve la reconnaissance faciale du fichier TAJ*, *La quadrature du Net*, 3 May 2022, available at: www.laquadrature.net/2022/05/03/le-conseil-detat-sauve-la-reconnaissance-faciale-du-fichier-taj.
[16] *Ibidem.*
[17] See Conseil d'État, Décision No. 447970, 4 January 2021, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-01-04/447970.
[18] See Decree No. 1511, 2 December 2020, amending the provisions of the *code de la sécurité intérieure* relating to the processing of personal data known as *Prévention des atteintes à la sécurité publique*, available at: www.legifrance.gouv.fr/jorf/id/JORFTEXT000042607323.
[19] *Ibidem.*
[20] Conseil d'État, Décision No. 447970, 4 January 2021, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-01-04/447970.

the aim pursued by the data controller. Consequently, the Conseil d'Etat also assessed the proportionality of the use of facial recognition for face matching purposes by the police in relation to the TAJ system consultation. The Conseil d'Etat considered that use of the system was sufficiently regulated and that it was proportionate as regards the aim pursued, i.e, crime prevention, investigation and repression.

In particular, the Conseil d'Etat considered that: "Facial recognition devices may only be used by the competent services in cases of absolute necessity, assessed solely in the light of the purposes of the processing operation, where there is doubt as to the identity of a person whose identification is required. This identification, assisted by this system, is the responsibility of the officials themselves. The regulatory provisions at issue, which govern only the use of [TAJ] are not intended to define the conditions for collecting images of people in public spaces or posted on social networks, nor to authorise the systematic or large-scale comparison of such images with the biometric templates stored in this processing. […] It follows that the contested processing operation contains appropriate safeguards for the rights and freedoms of the data subjects and does not, contrary to what is claimed, establish a 'disproportionate mechanism'".[21]

It is worth noting that the Conseil d'Etat assessed the proportionality of this specific use of facial recognition for criminal investigations by comparing it with other ways in which facial recognition is used by law enforcement agencies. The Conseil d'Etat therefore seemed to be making a distinction between using it in this specific way and using facial recognition in "real-time" when deploying systems in public places that match all bystanders' faces with the faces of people who appear in a particular watchlist. [22] The Conseil d'Etat stated in this respect that "[t]he regulatory provisions at issue, which govern only the use of the [TAJ], are not intended […] to authorise the systematic or large-scale comparison of such images with the biometric templates recorded in this processing".[23]

Similarly, the Conseil d'Etat considered that the provisions that concern the TAJ database "are not intended to define the conditions for collecting images of people in public spaces or posted on social networks".[24] Such systems may encompass systems such as Clearview AI software which has been deemed unlawful by many Data Protection Authorities (DPA) across Europe.[25]

With these considerations taken into account, the Conseil d'Etat concludes that "the contested processing operation contains appropriate safeguards for the rights and freedoms of the data subjects and does not, contrary to what is claimed, establish a 'disproportionate mechanism'".[26]

The Judges' reasoning suggests that the purpose of Article R 40-26 of the Code of Criminal procedure is not to authorise large-scale face matching devices or to authorise facial recognition systems such as Clearview AI, which provides law enforcement agencies with a database of images of individuals taken from the open web and notably from social networks. The Conseil d'Etat seems to acknowledge that the TAJ system is provided for by legal provisions and is less intrusive than other approaches, such as the automated processing of images from social media or the large-scale deployment of facial recognition devices.

5. *The Conseil d'Etat's decision from a comparative perspective*

The Conseil d'Etat's decision comes at a time of great debates in Europe about the use of facial recognition technologies in general and the specific way in which these

[21] Conseil d'État, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

[22] We categorise this kind of systems as "Large-scale face matching use-cases", see T. Christakis, K. Bannelier, C. Castelluccia and D. Le Métayer, *Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification*, Report of the AI-Regulation Chair (AI-Regulation. Com), MIAI, May 2022.

[23] Conseil d'Etat, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

[24] *Ibidem*.

[25] See for instance, ICO, *Enforcement Powers of the Information Commissioner: Monetary Penalty Notice*, available at: https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/, or CNIL, Décision MED-2021-134 du 26 novembre 2021, available at: www.legifrance.gouv.fr/cnil/id/CNILTEXT000044499030, last accessed on 7 April 2022.

[26] Conseil d'Etat, Décision No. 442364, 26 April 2022, available at: www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

technologies are used by law enforcement agencies in particular. The Conseil d'Etat's decision should therefore also be interpreted in the context of these debates. We would like to make four series of observations in this respect.

1) First, it should be noted that law enforcement authorities in Europe are increasingly using new technologies in general and facial recognition in particular in order to identify suspects. According to the TELEFI project study, as of the date of December 2020 facial recognition had been implemented in a similar way to the French TAJ system in 10 other EU Member States (Austria, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, The Netherlands and Slovenia), in the UK and by Europol and Interpol. 7 EU Member States (Croatia, Cyprus, Czech Republic, Estonia, Romania, Spain and Sweden) had reached the stage of preparing for implementation, and they were expected to start using the technology within one to two years.[27] While the legal landscape concerning the use of facial images in criminal investigations varies significantly from one EU country to another, all of these countries are subject to the "strict necessity" and proportionality requirements of the LED. From this point of view the decision of the Conseil d'Etat could reinforce the argument about using facial recognition to support criminal investigations in Europe.

2) It should also be noted that the Conseil d'Etat's decision is not the first time that the "strict necessity" and proportionality of the use of facial recognition to support criminal investigations has been assessed in Europe. As a matter of fact, a few DPAs and Courts in EU Member States and the UK have already had the opportunity to adopt a position on this issue.

A decision of particular relevance to this issue was issued by the 'Garante per la protezione dei dati personali', the Italian DPA. As a matter of fact, the Italian police use a system called "SARI-Enterprise" which basically enables police officers to match the photograph of a suspect with the AFIS-SSA database. In this respect the system is very similar to the French TAJ system. When analysing the lawfulness of such a system, the Italian DPA stated that it was "a mere assistance to human action".[28]

In other words, both the "Conseil d'Etat" and the "Garante" considered that given that the facial recognition systems were used as a mere assistance to police work, the LED's "strict necessity" requirement would be met.

3) The third series of observations concerns the relationship between the issue being considered by the Conseil d'Etat and the legislative work currently being undertaken by the EU Institutions regarding the EU Commission's proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act).[29] Article 5 of the draft regulation includes, in the list of prohibited AI practices, "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement"[30] except when these systems fulfil certain specific, listed purposes. However, these "Real-Time biometric identification systems" do not cover systems such as the TAJ since the latter is not intended to be deployed in real-time. The AI Act proposal does not therefore prohibit biometric ex-post identification of individuals for criminal investigation purposes. Nonetheless, such systems will be submitted to the pre-market requirements imposed by the draft AI Act.[31]

4) A final series of observations concerns the relationship between the Conseil d'Etat's decision dated 26 April 2022 and the first version of the Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted by the European

[27] See the *Summary report of the project 'Towards the European Level Exchange of Facial Images*, *Telefi Project*, Version 1.0, January 2021, 10, available at: www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf.

[28] Garante per la Protezione dei Dati Personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 July 2018, available at: www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9040256.

[29] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, com/2021/206 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[30] *Ibidem*.

[31] See T. Christakis, *Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021*, 27 May 2021, available at: https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021.

Data Protection Board on 12 May 2022 and consequently submitted for public consultation.[32] According to the EDPB, "such tools should be used in strict compliance with the applicable legal framework and only in cases where they satisfy the requirements of necessity and proportionality […] while modern technologies may be part of the solution, they are by no means a 'silver bullet'".[33]

The EDPB specifies the conditions under which a facial recognition system used for investigation purposes may be considered lawful. In particular, the EDPB states that "[t]he national law must be sufficiently clear in its terms to give data subjects an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such measures".[34] Furthermore, as regards the necessity requirement, the EDPB considers that "[p]rocessing can only be regarded as 'strictly necessary' if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary. […] This requirement should be interpreted as being indispensable".[35] As mentioned previously, LQDN claimed that the reasoning of the Conseil d'Etat was flawed because something that is perceived as providing mere assistance should not, in their opinion, be considered indispensable.

In view of the above, it remains to be seen whether NGOs such as LQDN will make use of these guidelines, and especially the specifications proposed by the EDPB for there to be law of sufficient "quality" and "special safeguards", in order to challenge, in future, the facial recognition provisions of the French Code of Criminal Procedure.

6. *Conclusion*

The Conseil d'Etat's decision reaffirms the validity of article R 40-26 of the code of criminal procedure, which expressly provides for the option to resort to facial recognition in criminal investigations. The Conseil d'Etat claims that using facial recognition in such a way is necessary when the amount of data available to the police is taken into account, and that it is proportionate to the aim pursued. This decision is part of a wider issue in Europe, where facial recognition for investigative purposes has been under the spotlight. Indeed, States are currently thinking about which facial recognition techniques should be prohibited and what facial recognition uses should be authorised, assuming that adequate safeguards are put in place. The view of the Conseil d'Etat, together with that of the Italian DPA, tends to suggest that States consider that deploying facial recognition for ex-post individual identification purposes is necessary and proportionate to the aim pursued, which is to repress crime. The EDPB and the draft AI Act also align in terms of allowing such deployments if there is an appropriate national legal framework providing proper safeguards.

[32] European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, 12 May 2022, available at: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.
[33] *Ibid*, 26.
[34] *Ibid*, 18.
[35] *Ibid*, 19.