

When the alarm comes from outside

Detecting, verifying and correcting police facial-recognition misuse in Sweden, Belgium and France

Tom Anciaux Berner, AEGIS · ORCID 0009-0006-1414-7400
Expert Review Edition · Version 1.0 · 27 October 2026

Research status. Source-based comparative pilot covering three Member States. It is not an EU-wide assessment and does not estimate the prevalence of unlawful processing.

Evidence standard. Factual statements are referenced to primary sources with page or paragraph numbers. Statements resting on secondary sources are marked as such. Evidence was collected up to 27 October 2026.

Edition. Released for expert review. Open items that must be resolved before a definitive edition are listed in section 11.

Abstract

European safeguards governing police use of facial-recognition technologies are commonly assessed through their legal design: statutory restrictions, prior authorisation requirements, data protection impact assessments, supervisory powers and judicial remedies.

This pilot examines a different question. When potentially unlawful biometric processing occurs, what makes it visible to oversight authorities, what evidence allows its extent to be independently reconstructed, and how can the implementation of corrective measures be demonstrated?

It examines four documented police facial-recognition uses or trials in Sweden, Belgium and France, and keeps a separate, unresolved French allegation as a research lead. In all four cases, the documented supervisory action followed a public report. In three, it was press coverage. In the fourth, the Brussels Airport system, it was a press interview in which the police commissioner-general announced the technology. The supervisor states that it was not aware of it, although the equipment had been acquired in 2017.

The evidence does not establish that national supervisory systems are ineffective. Once informed, supervisors investigated, established breaches, imposed corrective measures and, in Belgium, halted a deployment. The evidence identifies specific limitations in the public demonstrability of oversight: incomplete reconstruction of historical use, reliance on information supplied by supervised organisations or by vendors, and limited public evidence that corrective measures were implemented. The Swedish case adds that the financial penalty was annulled on appeal.

The study argues that the existence of legal safeguards, their operational effectiveness and the ability to demonstrate that effectiveness must be assessed separately.

1. Research question and scope

The central research question is: *can European supervisory authorities demonstrate that safeguards governing police facial recognition operate effectively when potentially unlawful processing occurs?* It is examined through four stages.

Stage	Question
S1 Visibility	How and when did the supervisory authority learn that the deployment existed?
S2 Establishment	How was an irregularity identified and legally established?
S3 Auditability	Could the actual extent of processing be independently reconstructed?
S4 Correction	Is there verifiable evidence that corrective measures were implemented?

The core pilot includes the Swedish police use of Clearview AI, the Belgian federal police use of Clearview AI, the Brussels Airport facial-recognition system, and the facial-recognition function of BriefCam in France. Allegations concerning facial matching against the French TAJ police records file through NEO mobile devices are retained as an unresolved research lead, not as an established finding.

These cases were selected because they are documented publicly. They are not a representative sample of police biometric processing in Europe. Events between 2017 and 2024 are assessed against the law applicable at the time, chiefly national legislation implementing Directive (EU) 2016/680. Obligations introduced later under the AI Act are not applied retroactively.

2. Methodology: separating occurrence, effectiveness and evidence

Each proposition is given one of four factual classifications:

Code	Meaning
P	Documented occurrence: the action, procedure or control is established by the evidence.
A	Documented absence: a competent source establishes that a required action or mechanism was not performed or did not exist.
I	Documented inability: a procedure or investigation occurred, but the record establishes that it could not resolve a specified question.
U	Insufficient public evidence: the public record does not establish the answer. U implies neither compliance nor failure.

These classifications are kept separate from the grade of the evidence: 1 for primary institutional records, 2 for secondary reporting, 3 for inference by the author.

For independent auditability, the study examines the provenance, integrity, retention and accessibility of evidence. Records held by a police organisation are not automatically unreliable, and records held by an external vendor are not automatically trustworthy.

Two registers are kept. Register A records documented incidents. Register B records institutional controls, including prior consultations, inspections and preventive interventions that did not lead to a public controversy. Search logs are maintained for each country.

Above all, the study separates three propositions that are frequently conflated: **a control was performed; a control was effective; its effectiveness can be independently demonstrated.** None of these automatically establishes the next.

3. Sweden: Clearview AI and the limits of the enforcement narrative

Between autumn 2019 and 3 March 2020, employees of the Swedish Police Authority used Clearview AI, a privately operated facial-recognition service, on a number of occasions, without the authority having provided the application [1, pp. 1-2].

Following media reports in February 2020 suggesting that Swedish law enforcement might have used the service, the Swedish data protection authority (IMY, then Datainspektionen)

immediately asked the police whether, and on what legal basis, it had done so [1, p. 2]. On 9 March 2020, the police press office publicly stated that it was not aware of any use within the authority [S1, secondary].

On 10 February 2021, IMY found breaches of the Swedish Criminal Data Act: biometric data processed without the required strict necessity, insufficient organisational measures, and no data protection impact assessment before use. It imposed a penalty of SEK 2.5 million and ordered training, information to the persons concerned, and measures to have the data deleted [1, pp. 1, 6-8]. IMY stated that it could not determine what had happened to the data uploaded to the service [1, pp. 7-8].

The judicial outcome

The judicial outcome materially changes the case. The Stockholm Administrative Court upheld the penalty on 30 September 2021 [2]. The Administrative Court of Appeal in Stockholm annulled that judgment and IMY's penalty decision on 7 November 2022 (case 7678-21). The Supreme Administrative Court refused leave to appeal on 17 November 2023 (case 6943-22) [3]. The financial penalty therefore cannot be presented as a finally upheld sanction.

According to a published summary, the appeal court considered that the deficiencies stemmed from individual employees' own actions rather than from shortcomings in the authority's routines [S3, secondary]. If the full judgment confirms this, it is directly relevant to this study: organisational safeguards would have been judged adequate while individual use bypassed them. The appellate judgment has not yet been examined in full. Until it is, no conclusion is drawn on whether IMY's findings on biometric data and impact assessment, or its non-financial orders, survived.

The case nevertheless establishes a visibility finding: IMY's investigation began after media reports, as IMY states in its own decision [1, p. 2]. It leaves open the number of searches, the fate of the uploaded data and the execution of the corrective measures.

A preventive counterexample

On 23 October 2019, the police submitted a separate, planned facial-recognition system, to be run against the national signalment register by the National Forensic Centre, for prior consultation [4, p. 1]. The authority advised that the retention period of the biometric feature vectors be settled before the activity began, describing this as an important part of the impact assessment [4, p. 3].

This shows that a preventive procedure was activated. It does not establish that the advice was implemented or that later processing complied with the law. The contrast is between a deployment brought into a formal oversight process and another use that became visible through external reporting. It does not show that preventive supervision as a whole was ineffective.

4. Belgium: Clearview AI and the limits of independent verification

The report of the Belgian Supervisory Body for Police Information (COC), DIO21006, approved on 4 February 2022, is publicly available [5]. It provides the pilot's most detailed evidence.

A member of the federal judicial police first used Clearview AI during a Europol Victim Identification Taskforce in The Hague, held from 14 to 25 October 2019, where participants from 24 countries saw the tool applied to data from the US National Center for Missing and Exploited Children [5, paras. 13-14, n. 37].

After a press article of 28 February 2020, the COC wrote on 2 March 2020 to the police committee responsible for information and ICT [5, para. 2]. The reply of 19 May 2020 stated

that the federal police had no organisational knowledge of any use of facial-recognition software [5, para. 3]. The COC accepted this and concluded that there had been no use [6, p. 4].

After a BuzzFeed News report of 25 August 2021, the COC wrote again on 27 August 2021 [5, paras. 1, 5]. The reply of 22 September 2021 admitted use by two members of the central directorate for serious and organised crime, contradicting the 2020 answer [5, paras. 5, 17-18]. The COC found that the unit had been informed verbally right after the taskforce, and in writing by 7 November 2019 at the latest [6, p. 6].

This sequence shows a specific supervisory vulnerability: an authority may activate its investigative powers yet remain dependent on the completeness and accuracy of information supplied by the organisation under examination.

The 78-search figure

The figure of 78 searches came from Clearview, in an e-mail of 16 September 2021 [5, para. 15, n. 44]. The COC states that it did not examine the accuracy of this information and could not do so, because the company falls outside its competence [5, n. 41]. It could not verify either the claim that the searches produced no positive result [5, n. 45], and on that point relied on the statements of the two investigators [5, para. 27]. No entries or logs of these uses were found in existing police databases [5, para. 27].

These are different evidentiary limitations. One concerns the reliability of a vendor's account of processing activity. The other concerns the operational consequences of that processing.

Legal findings and corrective measures

The COC found that the Police Function Act does not regulate facial recognition or the disclosure of police data to a private actor of this kind [5, para. 21]. Photographs were transferred to a US company without an adequacy decision or an applicable exception, which the COC treats as a data breach [5, para. 22]. An impact assessment should have been carried out before use, and the COC had no information that one was [5, para. 24].

The COC ordered the federal police to meet its data-breach obligations, including asking Clearview to delete the photographs supplied and the related biometric templates and raw data, with proof of compliance due within two months. It also warned that any future use of Clearview or similar tools would be unlawful [5, conclusions]. The order is documented. The assembled record does not establish whether satisfactory proof of deletion was supplied. The COC's 2022 activity report does not mention the follow-up [7].

The cross-border dimension

A letter from the commissioner-general, cited in the COC report, states that trial licences were provided by Europol to the taskforce participants [5, p. 5]. The report does not establish how this access was arranged. Swedish use also included a Europol meeting in The Hague in autumn 2019, according to the Swedish police as reported by the press [S2, secondary].

This is a concrete research lead on how commercially supplied biometric tools enter operational police environments. It does not establish that Europol authorised the later uses, that the Swedish and Belgian cases arose from the same event, or that any coordinated deployment existed. Those questions require separate investigation.

5. Belgium: Brussels Airport, a deployment the supervisor did not know about

In an interview published by the weekly Knack on 10 July 2019, the police commissioner-general announced that facial recognition would be used at Brussels Airport. The COC states that it was not aware of the technology, and requested information the same day. It

received a reply on 18 July 2019 and visited the airport police on 9 August 2019 [8, para. 2].

The COC found four cameras, purchased in early 2017 by the airport operator for the airport police. Snapshots were compared with internally compiled lists, and a match produced a hit. Testing had stopped in March 2017 because of a very large error margin. At the time of the visit the system was still partly active: snapshots of passers-by were still being taken, but no longer compared [8, paras. 4-7].

The COC was not convinced that the Police Function Act provided a basis, and found that storing biometric snapshots would create a technical biometric database that was not legally possible at the time [8, para. 9]. On 16 September 2019, it imposed a corrective measure temporarily ending the processing of biometric data, with confirmation to be sent to the COC [8, section 6]. The interim report does not expressly order deletion of the stored snapshots and contains no follow-up [8, paras. 7, 11]. In May 2020, the minister confirmed in Parliament that the project had been interrupted following the COC's opinion [9]. The COC's 2022 activity report records the case as ended by a corrective measure [7, p. 38].

This case was initially considered a potential counterexample, in which supervision would have operated outside the pattern of press exposure. The COC's report does not support that reading. The supervisor learned of the system through the press, from the operator's own announcement, about two and a half years after the equipment was acquired. The case does show something different and important: once informed, the supervisor visited within a month and halted the biometric processing within ten weeks.

6. France: BriefCam and the reconstruction of historical processing

French authorities examined the use of BriefCam video-analysis software after investigative reporting published by Disclose on 14 November 2023. The minister ordered an inspection on 24 November 2023, and the CNIL opened a review on 6 December 2023 [10, p. 5]. The CNIL also had a pre-existing strategic priority on automated image-analysis technologies for 2022 to 2024 [11]. The later controls must be read in the context of both that prior planning and the specific media disclosure.

BriefCam offers several video-analysis capabilities, and this study does not equate them with biometric identification. The vendor added a facial-recognition function in November 2018 [10, p. 29, n. 48]. The core corpus is limited to the documented use of that function in a judicial investigation, which the inspection report characterised as outside the applicable legal framework [10, p. 6].

The national police filed its compliance commitment for BriefCam with the CNIL on 14 December 2023, after the press article [10, p. 32]. The CNIL found that commitments of this kind had been sent late, sometimes years after deployment, or not at all [11].

The evidentiary limitation

Connection logs were deleted after 365 days. The inspectors therefore relied on the declarations of the services concerned to reconstruct historical use [10, p. 6]. This is a limitation of the audit trail available to the investigation. It does not establish that no other technical records could have existed.

On 15 November 2024, the CNIL issued formal notices requiring, among other things, the missing compliance commitments and impact assessments, and the removal or restriction of the facial-recognition function [11]. The assembled public evidence does not establish that all corrective measures were implemented and closed.

7. France: the unresolved TAJ and NEO allegations

Reporting published by Disclose on 16 March 2026 raised concerns about facial matching against the TAJ police records file through NEO mobile devices during identity checks. Several written parliamentary questions followed, none of which had received a ministerial answer by 27 October 2026 [13]. These allegations warrant investigation, but they must remain separate from established supervisory findings.

An earlier warning by the French police inspectorate (IGPN) in its 2023 report, on frequent consultation of the TAJ during identity checks, concerns consultation of the file in general, according to the parliamentary questions that cite it [13]. It cannot be treated as evidence that the inspectorate identified facial-recognition misuse. The 2023 report itself has not been examined. The IGPN's 2024 report links misuse of police files to the rollout of NEO devices and records 76 investigations for file misuse, without mentioning facial recognition [12, pp. 21, 28]. Aggregate TAJ consultation volumes cannot be presented as facial-search volumes, and the published figures are described inconsistently.

Until the original administrative records, instructions and any supervisory findings are obtained, the case remains provisional. Its inclusion in the research agenda does not make it a fifth established violation.

8. Institutional controls: what the preventive register shows

Register B records controls that did not necessarily lead to a public controversy. It is not yet exhaustive. The entries assembled so far are these.

Country	Control	Source
Sweden	Prior consultation on a planned police facial-recognition system, October 2019 (section 3).	[4]
Sweden	On-site inspection of biometric border control at Arlanda airport, with a reprimand for insufficient information to travellers. Contextual: fingerprints and verification, not facial identification.	[15]
Belgium	COC supervisory investigations are mostly opened ex officio.	[7, p. 45]
Belgium	28 impact assessments on police camera use submitted to the COC in 2022; most received comments or binding conditions.	[7, pp. 36-37]
Belgium	Published COC reports from 2020 to 2026 include thematic supervision of drones and police cameras. DIO19005 and DIO21006 are the only ones on facial recognition.	[14]
France	CNIL control priority on automated image analysis, 2022 to 2024.	[11]
France	IGPN detection of police file misuse: 76 investigations in 2024, disciplinary findings against 33 agents.	[12, pp. 21, 28]

These entries document different forms of preventive and proactive oversight, but do not establish their effectiveness in detecting undeclared facial-recognition deployments. The assembled record contains no instance in which such a control detected an undeclared facial-recognition use before public reporting. The COC states this limit itself, with regard to cameras: it has no or insufficient view of camera use that is not visible to it, and suspects a substantial dark number [7, p. 35]. It also reports having had no IT specialist from 1 August 2022 [7, p. 30].

9. Comparative findings

Finding 1. In all four established cases, documented supervisory action followed a public report. In Sweden, Belgium (Clearview) and France, it was press coverage [1, p. 2; 5, para. 2; 10, p. 5]. At Brussels Airport, it was the operator's own announcement in a press interview, about a system the supervisor did not know about [8, para. 2]. External disclosure

can activate meaningful supervision. This does not establish that proactive supervision was absent or ineffective in other cases.

Finding 2. The documented preventive procedures were activated for processing brought within their scope. Prior consultation and impact-assessment review are documented in Sweden and Belgium. The four established cases concern uses that did not pass through these procedures: two through a commercial service the police organisation had not provided [1, p. 2; 5, p. 5], one on equipment acquired in 2017 and unknown to the supervisor [8, paras. 2, 5], and one through a function added by a software update [10, p. 29, n. 48]. This is an observation on four cases and a hypothesis for further research, not a European finding.

Finding 3. Establishing unlawful processing does not establish its full extent. Different questions need different evidence: how many searches occurred, who conducted them, which images were uploaded, what results were obtained, and what happened to the data afterwards. The Belgian report shows this most clearly, because it separates information supplied by the vendor from facts the supervisor could verify [5, nn. 41, 44, 45].

Finding 4. Corrective orders and verified correction are different outcomes. The pilot documents investigations, formal notices, orders and the interruption of a deployment. For none of the corrective measures does the assembled public record establish final implementation. This is a limitation of the evidence, not proof that the measures were ignored.

Finding 5. Enforcement outcomes must be followed through the whole judicial process. The Swedish penalty, upheld at first instance, was annulled on appeal [3]. Research on the effectiveness of supervision must track appeals and final outcomes, not stop at the original regulatory announcement.

10. Institutional implications and limitations

Implications

Deployment visibility. Supervisory arrangements should account for trials, temporary access, free commercial accounts, software updates that add new functions, and technologies introduced outside ordinary procurement channels.

Technical traceability. Records should allow authorised reviewers to reconstruct relevant processing, subject to legal safeguards, retention rules and operational confidentiality.

Vendor accountability. Where biometric processing depends on external providers, supervisors may need reliable means of verifying account activity, transfers, retention and deletion.

Corrective transparency. Authorities could publish, where lawful and proportionate, information confirming the implementation or closure of corrective measures.

Judicial outcome tracking. Enforcement reporting should distinguish the original administrative findings, later judicial decisions and the final legal position.

These are implications drawn from the cases, not findings that current national systems lack the corresponding safeguards.

Limitations

First, the cases were selected because enough public information existed to reconstruct them, which biases the corpus towards publicised controversies. Second, the register of institutional controls is incomplete. Third, the study has no access to compliance correspondence, vendor records, inspection annexes or internal police audit trails. Fourth, the cases concern different technical systems and legal contexts: live identification, retrospective matching, verification

and general video analytics are not interchangeable. Finally, the pilot cannot estimate the prevalence of unlawful biometric processing or the detection rate of European supervisors.

11. Open items before a definitive edition

#	Item	Why it matters
1	Full judgment of the Administrative Court of Appeal in Stockholm, case 7678-21, 7 November 2022.	Determines which of IMY's findings and orders survived (section 3).
2	Documents filed after 10 February 2021 in IMY case DI-2020-2719; COC follow-up on DIO21006; any CNIL closure of decision MED-2024-150.	Necessary to assess implementation of several corrective measures.
3	COC follow-up on DIO19005, including the fate of the stored snapshots.	S4 for Brussels Airport.
4	IGPN annual report 2023, p. 35, and the Senate record of 1 April 2026.	Primary basis for section 7.
5	Systematic completion of Register B for all three countries.	Corrects selection bias towards publicised cases.
6	Independent review by a specialist in EU police data protection law and an audit-methods researcher.	Validation before institutional use.

Conclusion

The question is not simply whether European law establishes safeguards for police facial recognition. It is whether, when those safeguards are tested, institutions can demonstrate how a deployment became visible, how its actual operation was established, and whether the resulting corrections were carried out.

The cases examined show meaningful supervisory interventions: investigations, formal notices, corrective orders and the interruption of a deployment. They also show that in each case the intervention began with a public report, and they reveal specific evidentiary limits on reconstructing biometric processing and on publicly verifying the remedies that followed.

The pilot's central contribution is therefore not a finding that European biometric oversight has failed. It is a framework for distinguishing the existence of safeguards, their operation, and the evidence available to demonstrate their effectiveness. That distinction offers a testable basis for further comparative research.

Annex. Evidence register A (incidents)

Codes: P occurred, A documented absence, I documented inability, U insufficient public evidence. Grade: 1 primary, 2 secondary, 3 inference. References in brackets.

Case	S1 Visibility	S2 Establishment	S3 Auditability	S4 Correction
SE-1 Clearview, Swedish police	Supervisor acted after media reports, Feb. 2020: P-1 [1, p. 2]. Internal escalation before the press: U.	Breaches found: P-1 [1]. Penalty annulled on appeal: P-1 [3]. Survival of other findings: U.	Extent rests on police replies: provenance P-1 [1, p. 2]. Fate of uploaded data: I-1 [1, pp. 7-8]. Number of searches: U.	Orders: P-1 [1]. Execution and status after appeal: U.
BE-1 Clearview, Belgian federal police	COC acted after press, 2 Mar. 2020: P-1 [5, para. 2]. Unit informed by 7 Nov. 2019: P-1 [6, p. 6]. Escalation to the COC: A-1 [6, p. 6].	First inquiry closed on an incorrect answer: I-1 [5, para. 3; 6, p. 4]. Established after second press report: P-1 [5].	Police logs: A-1 [5, para. 27]. Search count supplied by vendor, not verifiable: I-1 [5, nn. 41, 44]. Results: I-1 [5, n. 45].	Deletion request and proof ordered: P-1 [5]. Execution: U [7].
BE-2 Brussels Airport system	COC learned from the commissioner-general's press interview; it was not aware: P-1 [8, para. 2].	No legal basis for a biometric database: P-1 [8, para. 9].	No logs or alert figures reported; error margin described as very large: U [8, para. 5].	Biometric processing halted: P-1 [8; 9]. Deletion of snapshots: U, not expressly ordered [8].
FR-1 BriefCam facial function	Controls after Disclose: P-1 [10, p. 5]. Commitments sent late or not at all: A-1 [11; 10, p. 32].	One use outside the legal framework: P-1 [10, p. 6].	Logs expired after 365 days: I-1. Count rests on declarations: I-1 [10, p. 6].	Formal notices: P-1 [11]. Execution: U.
FR-2 TAJ facial matching on NEO (provisional)	Press, 16 Mar. 2026: P-2 [13].	No authority finding: U.	Volume figures inconsistent: U.	U.

References

Primary sources

- [1] Datainspektionen (now IMY), Beslut efter tillsyn enligt brottsdatalogen, Polismyndighetens användning av Clearview AI, DI-2020-2719, 10 February 2021. <https://www.imy.se/link/5d5e59d4e64c4dcd909c0f7d42606960.aspx>
- [2] Förvaltningsrätten i Stockholm, judgment of 30 September 2021, case 4756-21. <https://www.publikt.se/sites/publikt/files/2021-10/Stockholm%20FR%204756-21%20Aktbil%2027%2C%20DOM%20-%20Integritetsskyddsmyndigh.pdf>
- [3] IMY, Tillsyn: Polismyndigheten, Clearview AI (case history: Kammarrätten i Stockholm, case 7678-21, 7 November 2022; Högsta förvaltningsdomstolen, case 6943-22, 17 November 2023). <https://www.imy.se/tillsyner/polismyndigheten/>
- [4] Datainspektionen, Förhandssamråd om Polismyndighetens planerade användning av programvara för ansiktsgenkänning mot signalementsregistret, DI-2019-10508, 23 October 2019. <https://www.imy.se/globalassets/dokument/ovrigt/2019-10-23-polisen-forhandssamrad.pdf>
- [5] Controleorgaan op de politionele informatie (COC), Toeziehtrapport met betrekking tot het gebruik van Clearview AI door de geïntegreerde politie, DIO21006, approved 4 February 2022. https://www.controleorgaan.be/files/DIO21006_Toeziehtrapport_Clearview_N_00050443.pdf
- [6] Belgian Chamber of Representatives, DOC 55 2716/001, 23 May 2022, report of the hearing of the COC of 9 March 2022. <https://www.lachambre.be/FLWB/PDF/55/2716/55K2716001.pdf>
- [7] COC, Activiteitenverslag 2022. https://www.controleorgaan.be/files/Activiteitenverslag_COC_2022.pdf
- [8] COC, DIO19005, interim report with corrective measure on facial recognition at Brussels Airport (airport police), approved 16 September 2019. https://www.controleorgaan.be/files/DIO19005_Onderzoek_LPABRUN_AT_Gezichtsherkenning_Publiek_N.PDF
- [9] Belgian Chamber of Representatives, CRABV 55 COM 175, Committee on Home Affairs, 11 May 2020. <https://www.dekamer.be/doc/CCRA/pdf/55/ac175.pdf>
- [10] Inspection générale de l'administration, Inspection générale de la police nationale and Inspection générale de la gendarmerie nationale, report on the use of BriefCam software, February 2024, published 28 October

2024. https://www.vie-publique.fr/files/rapport/pdf/296273_0.pdf

- [11] CNIL, Utilisation de BriefCam et de logiciels d'analyse vidéo par l'État et des communes : la CNIL prononce plusieurs mises en demeure, 5 December 2024 (decision MED-2024-150 of 15 November 2024). <https://cnil.fr/fr/utilisation-briefcam-logiciels-analyse-video-par-etat-communes-la-cnil-prononce-plusieurs-mises-en-demeure>
- [12] Inspection générale de la police nationale, Rapport annuel 2024. <https://www.vie-publique.fr/files/rapport/pdf/300479.pdf>
- [13] Assemblée nationale, written questions no. 14327 and 14328 (14 April 2026), no. 15003 (12 May 2026), no. 16976 (14 July 2026), no. 17894 (1 September 2026). <https://questions.assemblee-nationale.fr/q17/17-14327QE.htm>
- [14] COC, list of published reports. <https://www.controleorgaan.be/nl/publicaties/rapporten>
- [15] IMY, Beslut efter tillsyn, Polismyndigheten, IMY-2024-2904, 3 July 2026. <https://www.imy.se/globalassets/dokument/beslut/2026/beslut-tillsyn-polismyndigheten.pdf>

Secondary sources

- [S1] SVT, report of 9 March 2020 on Swedish authorities and Clearview AI. <https://www.svt.se/nyheter/inrikes/flera-svenska-myndigheter-vagrar-svara-om-appen-clearview-ai>
- [S2] SVT, report of 19 May 2020 on the police statement to Datainspektionen. <https://www.svt.se/nyheter/inrikes/nya-uppgifter-svensk-polis-anvande-kritiserade-ai-tjansten-fler-ganger-an-tidigare-kant>
- [S3] Qnister, Kamarrätten upphäver IMY:s beslut om sanktionsavgift, 24 November 2022. <https://www.qnister.com/kunskap/kamarratten-upphaver-imys-beslut>

None of the sources cited carries a DOI. All links were checked on 27 October 2026.