Law Enforcement Directive Implementation Country Report: France

Alexis Fitzjean Ó Cobhthaigh and Bastien Le Querrec

EDRi
European Digital Rights

Law Enforcement Directive Implementation Country Report: France

Alexis FitzJean Ó Cobhthaigh and Bastien Le Querrec

https://afocavocat.eu

TABLE OF CONTENTS

FULL DISCLOSURE

This report has been written by Alexis Fitzjean Ó Cobhthaigh, attorney at the Paris Bar, and Bastien Le Querrec, legal officer at the NGO *La Quadrature du Net* (LQDN), with the invaluable assistance of Cosmo Wenman, to whom the authors would like to extend the warmest thanks. Alexis often represents the NGO *La Quadrature du Net* and several other NGOs before French and European Courts, and he is also a member of *La Quadrature du Net*. This report is based on several *La Quadrature du Net* cases.

Introduction

The Law Enforcement Directive (LED) is primarily transposed[1] in Title III[2] (Articles 87 to 114) of the French Data, Records, and Freedoms Act of 6 January 1978[3] (hereafter the "French Data Protection Act" or the "French Act"), as amended by the French Ordinance of 12 December 2018,[4] and by Title III[5] (Articles 129 to 132) of the Implementing Decree n° 2019-536 of 29 May 2019. The designated data protection authority is the *Commission nationale de l'informatique et des libertés* (CNIL).

Prepared within the framework of an initiative coordinated by the NGO European Digital Rights (EDRi),[6] this report examines the transposition and implementation of the LED in France.

This report follows a similar structure to the initiative's other shadow reports. After focusing on data subject rights (Section I), sensitive personal data and the requirement for strict necessity (Section II), it will review the alignment of the legal bases for data processing and transparency (Section III), and changes in the law concerning new technologies and big data in relation to the LED (Section IV). This report is based on the review of laws, cases and secondary sources such as reports and studies.

[1] There does not seem to be any complaint, case-law, or formal opinions challenging the way the LED is formally transposed in French law.
[2] https://www.legifrance.gouv.fr/loda/id/LEGISCTA000037817613
[3] Free translation from French "*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*", available here: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/
[4] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037800506/
[5] https://www.legifrance.gouv.fr/loda/id/LEGISCTA000038567754
[6] https://edri.org/

Section I: Data subjects' rights

Chapter III (Articles 104 to 111)[7] of Title III of the French Data Protection Act relates to data subjects' rights. Article 104 of the French Data Protection Act relates to the information to be made available or given to the data subject. Article 104§I[8] of the French Act formally transposed Article 13(1) LED, and Article 104§II formally transposed Article 13(2) LED. Article 105 of the French Act relates to the right of access by the data subject, and formally transposed Article 14 LED. Article 106 of the French Act, relating to the right to rectification or erasure of personal data and restriction of processing, formally transposed Article 16 LED. The texts of Article 104 and Article 105 of the French Act closely track Article 13 and Article 14 LED, respectively. The provisions of Article 13(3) and Article 16(4) LED are faithfully transposed in Article 107§I[9] of the French Act. The French Data Protection Act's conditions are the same as those provided for by Article 13(3) and Article 16(4) LED.

As will be shown below, in the majority of instances, the statutory language of the French Act adheres closely to the wording of the LED.

Article 104§I of the French Act provides that the controller[10] has to make the following information available to the data subject:[11]

> 1° the identity and the contact details of the controller and, where applicable, of their representative;
>
> 2° the contact details of the data protection officer, where applicable;
>
> 3° the intended purposes of the processing of the personal data;
>
> 4° the right to lodge a complaint with the CNIL, and the contact details of the Commission;
>
> 5° the existence of the right to request, from the controller, access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

Article 104§II of the French Act provides that, in addition to the information referred to in paragraph I, in specific cases, the controller has to give the data subject the following additional information to enable the exercise of his or her rights:

[7] https://www.legifrance.gouv.fr/loda/id/LEGISCTA000037817682
[8] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037817684
[9] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037817690
[10] Article 3(8) LED defines the controller as "the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".
[11] Free translation from the original French.

1° the legal basis for the processing;

2° the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

3° where applicable, the categories of recipients of the personal data, including in countries outside the EU or within international organisations;

4° where necessary, further information, in particular when the personal data are collected without the knowledge of the data subject.

Article 105 of the French Act provides that the data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1° the purposes of and legal basis for the processing;

2° the categories of personal data concerned;

3° the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in countries outside the EU or within international organisations;

4° where possible, the expected period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

5° the existence of the right to request, from the controller, rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

6° the right to lodge a complaint with the CNIL and the contact details of the Commission;

7° communication of the personal data undergoing processing and of any available information as to its origin.

Article 106§I of the French Act provides that the data subject has the right to obtain from the controller:

1° the rectification of inaccurate personal data relating to him or her, without undue delay;

2° the completion of incomplete personal data including by means of providing a supplementary statement;

3° the deletion of personal data concerning him or her without undue delay when processing infringes the provisions adopted pursuant to the French Act, or when personal data must be deleted in order to comply with a legal obligation to which the controller is subject;

4° to restrict the processing in the cases pursuant to Article 106§III of the French Act.

Article 106§II of the French Act provides that, when the data subject so requests, the controller must provide evidence that it has carried out the operations required under Article 106§I.

Article 106§III of the French Data Protection Act provides that instead of deletion, the controller shall limit the processing when either:

> 1° the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained;
>
> 2° the personal data must be maintained for the purposes of evidence.

When processing is restricted pursuant to Article 106§III(1), the controller shall inform the data subject before lifting the processing restriction.

Article 106§IV of the French Act provides that the controller has to inform the data subject of any refusal of rectification or erasure of personal data, or restriction of processing, and the reasons for the refusal. It should be noted that while Article 16(4) *in limine* of the LED requires that such disclosure to the data subject must be "in writing", the French provisions do not specify which form it must take. In practice, however, it seems that in most, if not all, cases such disclosures are delivered in writing.

Article 106§V of the French Act provides that the controller has to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originated.

Article 106§VI of the French Act provides that when personal data has been rectified or deleted, or when processing has been restricted pursuant to Article 106§I or Article 106§III, the controller must notify the recipient[12] of the data of what must be done with the data.

Article 107§I of the French Data Protection Act provides that the rights of the data subject may be restricted, in accordance with the conditions laid down in Article 107§II of the French Act, to the extent that, and for as long as, such restriction constitutes a necessary and proportionate measure in a democratic society with regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

> 1° avoid obstructing official or legal inquiries, investigations or procedures;
>
> 2° avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
>
> 3° protect public security;
>
> 4° protect national security;
>
> 5° protect the rights and freedoms of others.

Any administrative order establishing a form of data processing must not only identify the data to be collected and the purpose of processing it, but also state if any of these five restrictions may be applied to it.

[12] While there is no specific definition of "recipient" given by the French Act, the last paragraph of Article 2 of the French Act provides that, except as otherwise provided, the definitions given by Article 4 of the GDPR apply within the scope of the Act. Since Article 4(9) of the GDPR gives the same definition for biometric data for unique identification as Article 3(10) of the LED, that definition is thereby incorporated into the French Act.

Article 107§II of the French Data Protection Act provides that, when the conditions laid down in Article 107§I are met, the controller may:

1° delay, restrict, or omit the provision of the information to the data subject pursuant to Article 104§II;

2° partially or completely restrict the right of access pursuant to Article 105 of the French Act. In such cases, according to Article 107§III, the controller must, without undue delay, inform the data subject of any refusal to rectify, delete, or restrict the processing of personal data, and the reasons for such refusals. However, the controller may forego such disclosures to the data subject when they would undermine a purpose under Article 107§I. In such cases, the controller must document the factual or legal bases for that decision and make that information available to the CNIL.

3° withold from the data subject any notification of refusals to rectify, delete, or restrict processing of personal data, as well as the reasons for those refusals, all of which would otherwise be required to be provided under Article 106§IV.

According to Article 107§IV, when a right has been restricted based on Article 107, the controller must inform the data subject of the possibility of exercising his or her rights through the CNIL. Except when a controller is lawfully delaying, restricting, or omitting the provision of the information to the data subject, the controller must also inform the data subject of the right to seek a judicial remedy.

Focus on the TAJ database case

The TAJ, which stands for *Traitement des antécédents judiciaires* (Criminal Records Processing), is a criminal records police database used in criminal and administrative investigations (e.g. search for criminal suspects, recruitment for sensitive jobs, etc.). In February 2022, the TAJ database contained more than 24 million files on natural persons, including 8 million that were anonymised.[13] **The management of the TAJ showcases systemic deficiencies in France's application of the data protection legal framework and data subjects' rights in the field of law enforcement.**

On 17 October 2024,[14] the CNIL delivered a decision concerning the TAJ database, finding several violations of the French Data Protection Act.[15]

First, the CNIL confirmed the *Conseil d'État*'s conclusion two years earlier[16] that the data processing of the TAJ police database falls within the scope of the LED, given the purposes of its processing schemes, which are the prevention, investigation, detection, and prosecution of criminal offences or the execution of criminal penalties.

Second, the CNIL found that the TAJ database practices were in violation of the principle of accuracy of data, as not every reasonable step had been taken to ensure that inaccurate personal data was erased or rectified without delay.

Third, the CNIL found violations of data subjects' right to information. More precisely, the Commission stressed that no provisions restricted the right to information of the data subjects, even though Article 107 of the French Act requires that any administrative order establishing a

[13] CNIL, 17 October 2024, n° SAN-2024-017, §5.
[14] CNIL, 17 October 2024, n° SAN-2024-017, §§ 10-21.
[15] Ibid.
[16] CE, 26 April 2022, ECLI:FR:CECHS:2022:442364.20220426.

form of data processing must not only identify the data to be collected and the purpose for processing it, but also state if any of the five possible restrictions apply to it. The CNIL noted that within the scope of Title III of the French Data Protection Act (transposing the provisions of the LED), the publication of generalised information could satisfy data subjects' rights to information, so long as that information was available without request and permanently accessible. The CNIL pointed out that data subjects are sometimes not even aware that their data has been processed by the TAJ database, and that for inmates or homeless people, general information published online was not truly accessible. In addition, for minors who may have their data processed by the TAJ database, information published online and in the Official Journal of the French Republic did not comply with the law, since it would require an affirmative action by an affected minor, and recital n°39 of the LED provides that "[s]uch information should be adapted to the needs of vulnerable persons such as children".[17]

Fourth, the CNIL found violations of access, rectification, and erasure rights: 777 applications for direct access rights to the TAJ database were pending on 31 December 2022, and 511 applications on 31 December 2023.[18] **The CNIL viewed this backlog as evidence of violations of data subjects' rights.**

Ultimately, the CNIL issued a formal reprimand to both the Ministry of Justice and the Ministry of the Interior, reminding them of their duties regarding articles 97, 104, 105, and 106 of the French Data Protection Act. The CNIL ordered them to bring the processing into compliance before 31 October 2026. In other words, the CNIL granted the ministers two years to comply with basic, essential data protection principles. It is difficult to conceive of a justification for such a delay, and indeed the CNIL provided no explanation.

Article 110 of the French Act goes beyond the rights introduced by the LED to access, rectify, or delete personal data, and actually grants any natural person the right to object, on legitimate grounds, to the processing itself of their personal data—except when the processing is legally required or when this right to object has been expressly ruled out by the order establishing the processing. This right to object to data processing is granted for methods of processing that fall within the scope of the LED, even while this right does not exist in the Directive itself. In practice, however, most of the acts that establish various forms of processing expressly rule out this right to object. We do not have sufficient data to examine how often individuals may exercise this right to object, if at all.

When personal data is processed on behalf of the State for the purpose of national security and defence, data subjects' rights to access, rectify, or delete personal data may be restricted pursuant to Articles 115 through 124 and Articles 140 through 151 of the French Act. France's compliance with Articles 15 and 17 LED is managed and supervised by the CNIL, which provides data subjects with an indirect right to access personal data that has been processed about them.

The CNIL is required to appoint as one of its members someone who serves, or has served, either the *Conseil d'État* (Administrative Supreme Court), the *Cour de cassation* (Civil and Criminal Supreme Court), or the *Cour des comptes* (Court of Auditors). It is this member's responsibility to investigate data subjects' requests and carry out the appropriate responses. The CNIL must then inform the data subject that all necessary verifications have taken place, as well as notify them of their right to seek a judicial remedy if they wish to challenge the CNIL's responses.

If the CNIL finds, in agreement with the controller, that the communication of a copy of the processed data in question would not prejudice the purposes of the processing—national security, national defence or public security—that data may be communicated to the data subject. However, if the controller is opposed to such communication, the CNIL has only to inform the data subject that it has made all necessary verifications.

The same applies to the right to rectification and erasure. While in some cases the CNIL and the

[17] "In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children."
[18] CNIL, 17 October 2024, n° SAN-2024-017, §75.

controller may be in agreement that a data subject's data should be rectified or deleted, and that the data subject should be informed, in other cases the controller may object to the CNIL's finding. In those cases, the CNIL will only inform the data subject that all necessary verifications have taken place,[19] without elaborating on any specific actions taken (such as exercising its corrective powers).

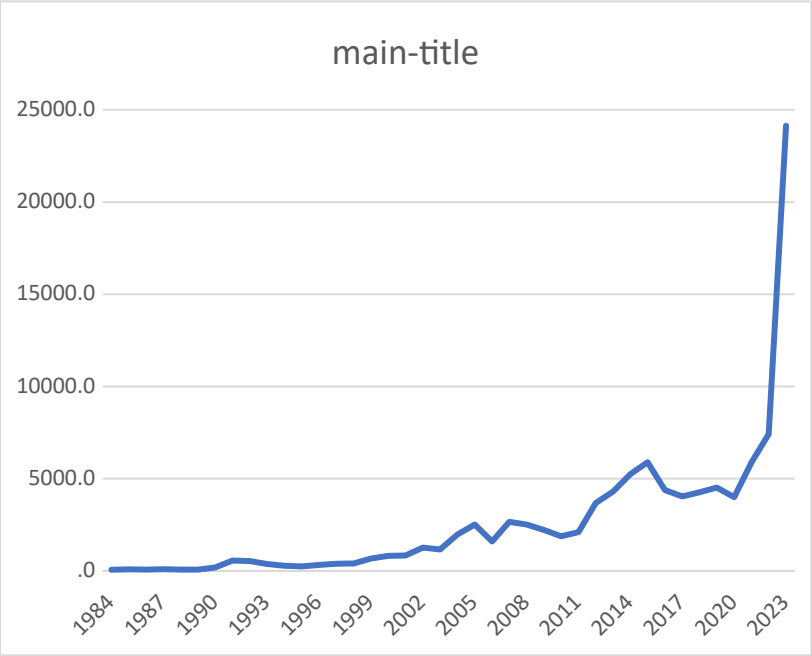
When a data subject disputes the CNIL's decision, the judicial remedy made available to them, as required by the LED, is for the subject to bring their dispute to court. Such cases that involve national security interests would be handled by a "specialised chamber" of the *Conseil d'État,* which consists of judges who have "national defence secret" clearance.[20] When national security is not an issue, ordinary administrative courts would hear the case. There are pending cases before the European Court of Human Rights (ECHR) regarding the compliance of this mechanism with the European Convention of Human Rights.[21]

Since some databases may contain data that relate to national security as well as data that do not, some disputes may be heard in part by the *Conseil d'État*'s specialised chamber for the elements that relate to national security, and in part by the ordinary administrative courts for the elements that do not, obliging a data subject to file two different kinds of lawsuits.[22]

The CNIL's annual report for 2023 states that the number of applications to access specific personal records has "skyrocketed",[23] from 6 555 requests in 2022 to 20 810 in 2023 (an increase of 317%). The CNIL dismissed 900 requests in 2022, and 1 600 in 2023. The Data Protection Authority carried out 5 800 inquiries in 2022, and 6 950 in 2023. The CNIL acknowledges that there has been a significant increase in the time it takes to process applications, and that in 2023, 1 600 applications had not been examined by the end of the year. The CNIL launched an online service in 2023 dedicated to responding to data subjects' requests to exercise their indirect right to access.

In its annual report for 2023, the CNIL anticipated a further increase in the number of requests in 2024, particularly in the context of the 2024 Olympic Games in Paris, no doubt related to the experimental—and purportedly temporary—deployment of several new mass surveillance technologies throughout the city during the games. Its annual report for 2024 states that the number of applications to access specific personal records reached 24 947 in 2024, and that it handled 14 654 requests.[24]

[19] CE, 10 November 2021, ECLI:FR:CECHR:2021:444997.20211110, §. 4.
[20] The list of processing methods subject to this specific procedure is laid down by article R. 841-2 of the Homeland Security Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049518814
[21] Case n° 40377/17, *Bodinier and others vs France*. More information available here: https://hudoc.echr.coe.int/eng?i=001-209962
[22] CE, 10 November 2021, ECLI:FR:CECHR:2021:444997.20211110, §. 6.
If the data subject files a lawsuit in the wrong jurisdiction (because it does not have competence on the case matter), that jurisdiction has to transfer the case to the competent one—except in summary proceedings.
[23] https://www.cnil.fr/sites/cnil/files/2024-05/cnil_44e_rapport_annuel_2023.pdf, p. 11.
[24] https://www.cnil.fr/sites/cnil/files/2025-04/rapport_annuel_2024.pdf, p. 9.



Sources: https://www.data.gouv.fr/fr/datasets/exercice-des-droits-indirect-donnees-generales/ (Open Licence 1.0: https://www.etalab.gouv.fr/wp-content/uploads/2014/05/Licence_Ouverte.pdf); *CNIL*'s 2023 annual report, p. 42; for the full data, see Annexes.

The significant increase in applications has occurred even though, in August 2018, the scope of the indirect right to access was narrowed to exclude several forms of data processing. In particular, criminal records held by police under the TAJ,[25] and national security, border control, and law enforcement records held by the Schengen Information System (SIS)[26] and the Wanted Persons Records (*Fichier des personnes recherchées* (FPR)) are excluded from the indirect right to access. Since then, data subjects may exercise a direct right to access personal data that has been processed about them in those three different processing systems (TAJ, SIS and FPR). We lack sufficient data to evaluate how, and how often, this direct right is actually exercised in practice.

Articles 37 and 38 of the French Act[27] transpose Article 55 of the LED, allowing third parties to aid data subjects. Non-profit associations or organisations that have been properly constituted in accordance with French law for at least 5 years and have as part of their stated purpose the protection of privacy and data subjects' rights and freedoms, may act on behalf of a data subject to exercise their rights to lodge a complaint and seek an effective judicial remedy against a supervisory authority; they may also seek an effective judicial remedy against a controller or processor[28] on the data subject's behalf.

Based on these provisions, the French NGO *La Quadrature du Net* (LQDN)[29] filed several complaints, including three on 24 September 2022 on behalf of 15 248 individuals,[30] against the TAJ[31] and TES[32] databases and their use of data collected from closed-circuit television systems (CCTV). Those complaints required the CNIL to ban surveillance cameras, facial recognition, and the gathering and use by police of a massive database of data subject information. According to LQDN, the complaint against CCTV was resolved by the CNIL in May 2024.[33] The other two complaints are still pending

[25] Article R. 40-33 of the code de procédure pénale (Criminal Procedure Code).
[26] Article R. 231-13 of the code de la sécurité intérieure (Homeland Security Code).
[27] Those articles belong to Title I of the French Data Protection Act, which applies to processing that falls within the scope of both the GDPR and the LED.
[28] Article 3(9) LED defines the processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".
[29] https://www.laquadrature.net/
[30] https://www.laquadrature.net/en/2022/09/30/15248-people-file-a-complaint-against-the-technopolice/
[31] CNIL, 17 October 2024, n° SAN-2024-017, §5.
[32] Acronym for *Titres électroniques sécurisés*, meaning "secured electronic documents".
[33] The decision was not published. According to LQDN, the complaint was rejected on the ground that the Interior Ministry, which was the public authority targeted in the complaint, could not be considered a joint controller of CCTV systems that are at the initiative of municipalities. The latter are considered the only

before the CNIL.[34]

The CNIL's processing of the three complaints based on the LED seems to follow a similar path as earlier examples filed by the same NGO and based on the GDPR, namely involving very lengthy decision-making processes. In 2018, for example, LQDN lodged five complaints with the CNIL on behalf of 12 000 individuals. Three of these (against Apple, Facebook and Google) are still being investigated by the Data Protection Commission (DPC) of Ireland through the "one-stop-shop mechanism". One of those has been only partially addressed by the CNIL (Google, concerning Android).[35] A fourth complaint led to a record fine (746 million euros) imposed by the Luxembourg DPA against Amazon,[36] which the Administrative Court of Luxembourg annulled by a judgment delivered on 12 March 2026.[37] The fifth complaint concerned the lawfulness, fairness and transparency of certain processing by LinkedIn, and, in October 2024,[38] led the DPC to issue a reprimand, an order to bring the processing into compliance, and an administrative fine totalling 310 million euros.

entities determining the purposes and means of data processing by CCTV and thus the sole controllers within the meaning of the GDPR, Article 4(7).

[34] Even though the CNIL delivered a decision on 17 October 2024 concerning the TAJ database, this decision did not follow the complaint filed by LQDN.

[35] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/

[36] https://www.laquadrature.net/2021/07/30/amende-de-746-millions-deuros-contre-amazon-suite-a-nos-plaintes-collectives/

[37] https://cnpd.public.lu/en/actualites/national/2026/03/arret-ca-amazon-cnpd.html

[38] https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million

Section II: Sensitive personal data and the requirement for strict necessity

The provisions of Article 10 LED are accurately transposed in Article 88[39] of the French Act. It therefore follows that the French law requires that the processing of sensitive data be "strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject" and that it occur only if authorised by French law, if its purpose is to protect the vital interests of a natural person, or if such processing relates to data that have manifestly been made public by the data subject.

Article 6§I[40] of the French Act faithfully transposes the list of sensitive data given by Article 9 of the GDPR and Article 10 of the LED. However, the legal basis in French law for processing that sensitive personal data is no more detailed or specific than it is for processing non-sensitive personal data. Article 88[41] of the French Act states only that processing sensitive data is possible "only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject". It must also be authorised by legislative or regulative provisions, or have as its purpose the protection of the vital interests of a natural person, or relate to data that are manifestly made public by the data subject. However, neither this Article nor any provision of the French Act identify what kind of "legislative provisions" are required. Article 31 of the French Act[42] could be read as providing that the processing of sensitive personal data must be authorised by decrees that have been informed by both the opinions of the *Conseil d'État* and the CNIL.[43] However, the letter of the French Act has been subject to diverging interpretations on this point.

Recently, the *Conseil d'État* handled two cases which, since they related to the processing of personal data about data subjects' health and disabilities, fell under the scope of the GDPR, and not the LED. In these cases, the *Conseil d'État* made a strict interpretation of the French Act, adopting a low threshold for satisfying the requirement for "legislative provisions". It considered, both in its advisory functions (in the General Assembly, administrative section)[44] and as a judge (in the litigation section),[45] that an ordinary decree requiring only the CNIL's opinion and not the *Conseil d'État*'s, would serve as a sufficient legislative basis for most forms of data processing.

Since French law makes no distinction on this point between the LED and GDPR, the *Conseil d'État*'s ruling confirms that simple decrees based only on the opinions of the CNIL may be

[39] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037817624
[40] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037822942
[41] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037817624
[42] *"I.- Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :*
1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;
2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.
L'avis de la commission est publié avec l'arrêté autorisant le traitement.
II.- Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement.
III.- Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.
IV.- Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation."
[43] Apart from its judicial functions, the *Conseil d'État* also exercises administrative and legislative functions, leading the European Court of Human Rights (ECtHR) to note that "the particular status of the *Conseil d'État* among French institutions connects it organically to the executive" (ECtHR, 9 November 2006, *Sacilor-Lormines v. France*, n° 65411/01, §. 66.)
[44] CE, AG (administrative section), 9 September 2021, opinion n° 403628.
[45] CE, 20 December 2023, *Association Act Up Paris*, ECLI:FR:CECHR:2023:468295.20231220

sufficient for most forms of processing to comply with the "legislative provisions" required by the LED.

Several more of the *Conseil d'État*'s views are apparent in its case-law. Often, the court will simply assert in a peremptory fashion that a form of processing is necessary, without explaining why,[46] even though both Article 10 LED and the rule of law require that the collection of sensitive data may be authorised only when adequate reasons for its "strict necessity" are given. The court also seems to conflate true necessity and *a fortiori* "strict necessity" with mere usefulness.[47]

Commenting in 2020 on a case it had just brought before the *Conseil d'État* opposing facial recognition data processing,[48] the French NGO *La Quadrature du Net* (LQDN) described the TAJ database as follows:

"This file contains, besides an overwhelming amount of information, images of people 'involved' in ... police investigations: convicted as well as acquitted individuals.

According to a report from the French Parliament[49] and the French data protection authority (the CNIL),[50] 19 million files and 8 million images are saved in this database.

Article R40-26 of the Code of Criminal Procedure[51] explicitly allows the police and the military to use facial recognition on these millions of images despite violating European data protection rules. As the CNIL explained in 2011,[52] this system makes it possible 'to compare the images of the faces of people involved in the perpetration of offences captured via CCTV devices with the photographs stored in the database', for example by comparing the face of a person filmed in the street by a camera with the photographs stored in the police databases in order to identify them. These techniques are already used[53] in current criminal affairs. Recently[54] with the Covid lock-down, strong suspicions of misappropriation of this database to levy fines against 'people known to the police' have come to light."[55]

Contemplating a program of such scale, the *Conseil d'État* ruled that processing sensitive personal data with the use of facial recognition systems was "strictly necessary" because the records in question contained photographs of several million people, a quantity that made it impossible to manually compare the images, and furthermore because manual comparisons could not be performed as reliably as with an algorithm. Furthermore, it found that the process of identifying a person from a picture of their face and comparing it to other collected data may be "strictly necessary" since it might fulfil the objective of preventing attacks on public order, and the constitutional objective of investigating perpetrators of criminal offences.[56]

---

[46] CE, 21 December 2021, ECLI:FR:CECHS:2021:442360.20211221, §. 7; CE, 24 December 2021, ECLI:FR:CECHR:2021:447518.20211224, §. 54: considers the question of whether personal data are kept in a form which permits identification of data subjects for "no longer than is necessary for the purposes for which they are processed"; CE, 30 December 2021, ECLI:FR:CECHR:2021:440376.20211230, §. 18 *in limine*.

[47] CE, 18 May 2020, ECLI:FR:CEORD:2020:440442.20200518, §. 13; CE, Ass., 21 April 2021, ECLI:FR:CEASS:2021:393099.20210421; CE, 12 December 2023, ECLI:FR:CEORD:2023:489923.20231212, §. 12.

[48] The author represented LQDN in this case.

[49] https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information.pdf

[50] https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires

[51] https://www.legifrance.gouv.fr/codes/id/LEGISCTA000025818428

[52] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025804888

[53] https://www.leprogres.fr/rhone-69/2019/11/01/la-reconnaissance-faciale-le-designe-il-est-condamne

[54] https://technopolice.fr/essonne/

[55] https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/; also available here: https://edri.org/our-work/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

[56] CE, 26 April 2022, ECLI:FR:CECHS:2022:442364.20220426, § 5:
"*5. En premier lieu, l'enregistrement dans le TAJ d'une photographie des personnes mises en cause comportant les données biométriques nécessaires à la mise en œuvre d'un dispositif de reconnaissance faciale a pour objet de permettre aux agents habilités à accéder à ce traitement et à procéder à ces opérations d'identifier une personne à partir de l'image de son visage, grâce à une recherche automatisée, et, le cas échéant, d'exploiter les informations de la fiche correspondante dans le TAJ, pour les finalités mentionnées à l'article 230-6 du code de procédure pénale. Eu égard au nombre de personnes mises en cause enregistrées dans ce traitement, qui s'élève à plusieurs millions, il est matériellement impossible aux agents compétents de procéder manuellement à une telle comparaison, de surcroît avec le même degré de*

The *Conseil d'État*'s interpretation of the "strictly necessary" condition seems to deviate significantly from the requirements of EU law, as most recently stated by the Court of Justice of the European Union in the *Ministerstvo na vatreshnite raboti* case (C-205/21)[57] of 26 January 2023 (§§. 116-135), which ruled, in part, that "the requirement that processing of sensitive data be 'strictly necessary' entails particularly strict checking, in that context, as to whether the principle of data minimisation is observed" (§. 125) and that "the requirement of necessity is met where the objective pursued by the data processing at issue cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (...). In particular, in the light of the enhanced protection of persons with regard to the processing of sensitive data, the controller in respect of that processing should satisfy itself that that objective cannot be met by having recourse to categories of data other than those listed in Article 10 of Directive 2016/680." (§. 126).

Moreover, in that same case, while the CJEU further ruled that "the 'strictly necessary' requirement means that account is to be taken of the specific importance of the objective that such processing is intended to achieve",[58] it did not rule that the amount of data is to be taken into account, nor the reliability of the processing.

Another case brought to the *Conseil d'État* by LQDN[59] also illustrates the *Conseil d'État*'s peculiar interpretation of the LED requirements. The case concerned GendNotes,[60] a mobile app developed by the government for use by police for the purpose of documenting their field observations and transmitting them more easily to a police database. The decree authorising the use of this application expressly called for police to use it to record information and individuals' personal data, including their names, gender, date of birth, country of birth, nationality, profession, physical address and email address, as well as their photograph and the circumstances of their arrest and alleged crime. Additional types of information could be recorded by typing free-form comments into a blank text field—at the police officer's discretion and based on their individual assessment made on the spot that this data collection is "strictly necessary". In practice, the app could thus easily collect and transmit information revealing subjects' race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning their health, sex life, or sexual orientation.

LQDN argued that the government's use of the GendNotes application did not meet requirements for strict necessity because of its open-ended comment field. This input method could indeed enable the police to gather any kind of sensitive data and automatically add it to any of its databases, regardless of its purpose. Firstly, the free-form comments section does not allow a distinction to be made between sensitive and non-sensitive data, which require different types of procedural safeguards. Secondly, compared to written form, the digitisation of police officers' notes and their transfer to other databases open the door to further processing for different, possibly incompatible, purposes. In addition, LQDN pointed out that the use of the application also failed the strict necessity test since the police were already perfectly capable of writing conventional notes and had previously functioned well without the app, which constitutes an alternative, comparably effective measure.

In his opinion on this case, the *rapporteur public,*[61] Alexandre Lallet, presented a contrary and rather expansive view of strict necessity and the consequences of upholding it, opposing LQDN's position by writing: "it is quite obvious that we cannot follow reasoning according to which the condition of

---

fiabilité que celui qu'offre un algorithme de reconnaissance faciale correctement paramétré. Or une telle identification à partir du visage d'une personne et le rapprochement avec les données enregistrées dans le TAJ peuvent s'avérer absolument nécessaires à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle. Par suite, l'enregistrement des données litigieuses dans ce traitement répond à la condition de nécessité absolue posée par les dispositions précitées."

[57] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62021CJ0205

[58] CJEU, 26 January 2023, *Ministerstvo na vatreshnite raboti*, case C-205/21, §. 127 *in limine*.

[59] The author of this report represented LQDN in this case.

[60] CE, 13 April 2021, ECLI:FR:CECHR:2021:439360.20210413

[61] The "*rapporteur public*" role is very similar to the Advocate General before the Court of Justice of the European Union (CJEU).

strict necessity [has not been] met since law enforcement can always record information in paper notebooks—otherwise, no automated processing will ever be necessary".[62]

The court was convinced by the government's argument that the police would only use the app in ways that were "strictly necessary" simply because the police were required by law to do so. However, it can be argued that, in practice, there are no effective controls of this compliance with the strict necessity principle and that the application is designed in a way that incentivises data collection, including sensitive data, beyond what is strictly necessary. The court also implicitly followed the *rapporteur public*'s position that the existence of a conventional alternative—even one as practical, effective, and well established as hand-written note-taking—obviously should be dismissed precisely because acknowledging it would undermine automated data processing in general.

If the "strict necessity" criteria could be based solely on the amount of data being collected or the unreliability of alternative means for processing it, any kind of collection and processing of personal data, by any means, could be justified as "strictly necessary" by the government. Indeed, it could simply scale up the collection operation or threaten to use less reliable alternative processing methods (such as in the *TAJ* case), or ignore or discard those alternatives altogether (in the *GendNotes* case). While that clearly would be contrary to the objectives of the LED, it is nonetheless the practical effect of the *Conseil d'État*'s decisions to date.

On 19 March 2026, the CJEU ruled that the LED precludes national legislation, such as the French one, which (i) provides for the systematic collection of the biometric data of any person reasonably suspected on one or more grounds of having committed or attempted to commit a criminal offence, unless it is established, first, that the national law defines the specific and concrete purposes pursued by that collection in an appropriate and sufficiently precise manner, and second, that the competent authority is required, in each individual case, to assess whether that collection is strictly necessary for achieving those purposes, so that that collection is not systematic; and (ii) does not lay down an obligation on the part of the competent authority to provide a sufficient statement of reasons, in each individual case, as to why it is "strictly necessary", within the meaning of that provision, to collect the biometric data of a person reasonably suspected on one or more grounds of having committed or attempted to commit a criminal offence.

This "*Comdribus*" case (case C-371/24)[63] concerned French law. The French criminal court that referred the case to the CJEU did not have the opportunity to rule on the case before it.

[62] Free translation from the original French, available at https://www.conseil-etat.fr/plugin?plugin=Service.downloadFilePagePlugin&Index=Ariane_Web&Id=/Ariane_Web/AW_CRP/%7C6169: "*il est bien évident qu'on ne peut suivre le raisonnement selon lequel la condition de strict nécessité ne sera jamais remplie puisque les gendarmes peuvent toujours consigner les informations sur les carnets papier – ou alors, plus aucun traitement automatisé ne sera nécessaire*".
[63] CJUE, 19 March 2026, *Comdribus*, n° C-371/24.

Section III: Alignment of the legal basis for data processing with the Law Enforcement Directive, transparency and accountability

Title V of the French Constitution governs relations between the French Parliament (National Assembly and Senate) and the French Government. Article 34 of the French Constitution confers on the Parliament exclusive competence relating specifically to legislative matters. Article 37 of the French Constitution provides that matters other than those coming under the scope of Article 34 shall be matters falling within the regulatory domain. In other words, the limits of the French Parliament's competence are governed by the principle of conferral of powers.

According to Article 21 of the French Constitution, the regulatory powers belong, save for those vested in the President of the French Republic, to the Prime Minister. The administrative acts issued by the Prime Minister (and by the President) are called "Decrees".

The Prime Minister delegates some of his powers to Ministers.[64] The Parliament may also delegate some powers to the Prime Minister, other Ministers (such as those at the Interior Ministry, Department for Culture or Foreign Affairs Office), or to local authorities such as mayors. The administrative acts issued by those administrative authorities are called "Orders". The administrative courts review the legality of these acts (Decrees and Orders) by hearing cases brought before them.

At the national level, several decrees and orders have been issued in attempts to fulfil the requirements of Articles 8 and 10 LED to provide a legal basis for each method of processing (sensitive) personal data.[65] However, other decrees and orders, notably those regulating criminal databases or surveillance methods, have not been updated swiftly after the formal transposition of the LED into French national law. Some of them were only brought in line with EU law once the data processing evolved or was reformed.[66]

Several orders have been issued at the local level as well, with the same objective of meeting Article 8 and 10 requirements. However, those orders are considerably less accessible than orders at the national level, in particular because local orders are only published in local collections of administrative orders, and often only after prolonged delays.

Such administrative orders allowing data processing (including drone and algorithmic surveillance, for example) are only published locally and on the prefects' websites—not at the national level, nor on a centralised website. Furthermore, these orders are often scanned from paper hardcopies and not processed by OCR, which renders keyword searching unfeasible, and makes it impractical to gather and monitor or analyse them in bulk.

LQDN developed Attrap,[67] a free and open-source research tool that automatically searches through local collections of administrative orders to index them, and that offers a web interface to search that database. LQDN's initial need was to automatically detect orders with keywords relating to algorithmic and drone-based surveillance, but the web platform allows anyone to look for any keyword or make precise searches. This tool helped LQDN demonstrate that such orders are often published only after the surveillance has already started. LQDN lodged a complaint[68] with the

---

[64] Article 21§2 of the French Constitution.

[65] Examples: Decree n° 2020-767 of 23 June 2020 establishing automated processing of personal data referred to as a "digital criminal record": https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042032044?fonds=LEGI&isAdvancedResult=true&page=1&pageSize=50&query=%7B%28%40ALL%5Bt%222016%2F680%22%5D%29%7D&tab_selection=all&typePagination=DEFAULT; Order of 7 April 2021 establishing the "PARCOURS" system for processing personal data: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000043344970?fonds=LEGI&isAdvancedResult=true&page=1&pageSize=50&query=%7B%28%40ALL%5Bt%222016%2F680%22%5D%29%7D&tab_selection=all&typePagination=DEFAULT

[66] Example: Article 251-1 of the Internal Security Code that regulated the use of videosurveillance was modified by the French Olympics Law to specify that videosurveillance implies personal data processing regulated by the GDPR and the French Data, Records, and Freedoms Act (which transposes the LED in its Title III).

[67] https://attrap.fr

[68] https://www.laquadrature.net/wp-content/uploads/sites/8/2024/07/Plainte-VSA-JO-LQDN-anonRS.pdf

CNIL in one case where the *préfet de police* (Police Commissioner) had authorised algorithmic surveillance from 26 July 2024 through 11 August 2024 by an order that had been made on 25 July 2024 but which had not been published until 30 July 2024, several days after the surveillance had already begun. Following this complaint, the CNIL reminded the Interior Ministry of its obligations in terms of the publication of its administrative orders, then closed the case.

In some cases where the law required surveillance to be authorised on a case-by-case basis, when locally justified, and constrained to specific locations and durations, the orders were published only after the surveillance had been completed. When the public cannot examine such orders and their legal bases, a judicial remedy is, by definition, not possible.

Answering a Freedom of Information Act (FOIA) request submitted to it by LQDN, the CNIL stated that, aside from scattered references in various French DPA reports,[69] the CNIL never received or produced any documents relating to predictive policing software.[70] LQDN observed that this notable lapse naturally "suggests that the agency had never taken any interest in such automated decision-making systems as part of its oversight powers. In and of itself, this raises important questions when considering that some of these systems are used by thousands of municipal police officers across France."[71]

These and many other examples have given rise to a broader criticism in France that the CNIL is failing to discharge its supervisory mandate.[72] This criticism should be viewed in light of responses the CNIL itself provided, on 11 December 2023, to questions from the European Commission about its report on the application of the GDPR under Article 97 of the said Regulation. The CNIL claimed that, despite substantial increases in its budget and human resources—from € 20 144 000 and 225 full-time employees in 2020 to € 27 900 000 and 298 full-time employees in 2024—its financial resources, human resources, and technical capabilities were nonetheless "insufficient".[73]

[69] https://cnil.fr/sites/cnil/files/atoms/files/cnil_cahiers_ip5.pdf
https://cnil.fr/sites/cnil/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
https://www.fnau.org/wp-content/uploads/2019/04/police_predictive.pdf
[70] https://madada.fr/request/1622/response/1593/attach/6/CADA%2022011583%20LIBREV%20CONSULTING.pdf?cookie_passthrough=1
[71] https://www.laquadrature.net/en/2024/01/18/predictive-policing-in-france-against-opacity-and-discrimination-the-need-for-a-ban/
[72] https://www.mesopinions.com/petition/droits-homme/cnil-rearmer-citoyens-dpo-face-aux/231045 ; https://demarches.asso-purr.eu.org/letters/f1a75962-9b68-4fad-a5a3-fa00ad090a57
[73] See §. 4.4.6: https://www.edpb.europa.eu/system/files/2023-12/fr_sa_gdpr_art-97questionnaire.pdf

Year	CNIL Budget (euros)	CNIL Staff (full-time equivalent)	Number of complaints received by CNIL (excluding requests for information)
2020	20 144 000	225	13 585
2021	21 507 000	245	14 143
2022	23 950 000	270	12 193
2023	26 029 549	288	16 433
2024	28 200 000	298	17 772

Sources: https://www.edpb.europa.eu/system/files/2023-12/fr_sa_gdpr_art-97questionnaire.pdf and https://www.cnil.fr/sites/cnil/files/2025-04/rapport_annuel_2024.pdf

Section IV: New technologies and big data

Since its adoption, the French Data Protection Act has been changed several times to meet the requirements of the LED and the GDPR. Article 11 LED is faithfully transposed in Article 95 of the French Act. More specifically, for example, Article 95§3 of the French Act closely follows the wording of Article 11(3) LED, stating that: "[p]rofiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 6§I shall be prohibited".

In practice, however, French law does not seem to take into consideration existing big data analytic practices in relation to the requirements introduced by the LED. Instead, it appears to focus on the supposed effectiveness and efficiency of the new technologies. In the following examples, basic data protection requirements such as the principles of legality, (strict) necessity, proportionality or data minimisation are undermined or ignored in favour of the experimentation and deployment of such techniques.

Mass algorithmic surveillance:

Article 10 of the 2023 French Olympic Games Act allows algorithmic processing of images and videos captured from closed-circuit television (CCTV) or drones, on an experimental basis and until 31 March 2025,[74] "for the sole purpose of ensuring the security of sports, recreational or cultural events which by their scale or circumstances are particularly exposed to acts of terrorism or serious attacks on the safety of individuals". The Act specifies that only "footage collected by CCTV or drones" in places hosting "sports, recreational or cultural events which by their scale or circumstances are particularly exposed to acts of terrorism or serious attacks on the safety of individuals" and surrounding areas, as well as inside public transportation systems and their means of access (e.g. train and subway stations), may be collected and processed by "algorithms".

The impact assessment accompanying the draft bill specifies that the algorithmic analysis of images is happening in real time and will detect certain abnormal events.[75] The Implementing Decree adopted on 28 August 2023[76] provides the list of categories of events to be detected: presence of abandoned objects; presence or use of weapons; failure by a person or vehicle to comply with the direction of traffic; crossing or presence of a person or vehicle in a prohibited or sensitive area; presence of a person on the ground after falling; crowd movement; excessive density of people; and outbreak of fire.

In terms of procedural safeguards, it is stated that:

- the use of algorithms is "strictly limited" as its only purpose is to ensure the security of public events;
- the amount of images algorithmically analysed is restricted (to those coming from CCTV and drones located in the venues and surroundings hosting the events);
- the targets of detection are limited to "pre-determined events" defined by the decree;
- the system excludes the use of biometric data and any use of biometric identification or facial recognition devices (see discussion in the following paragraph);
- the processing operations may not, on their own, carry out any automated reconciliation, interconnection or linking with other personal data processing operations;
- the CNIL must deliver an opinion, and the data controller must carry out a data protection impact assessment;
- the Interior Ministry must deliver a certificate before the use of an algorithmic system confirming its compliance with legal requirements, including the "relevance, adequacy, representativeness, fairness and objectivity of the

[74] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000046777392/
[75] https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/ei_art_39_2022/ei_-spox2233026l_cm_22.12.2022.pdf
[76] Decree n° 2023-828 of 28 August 2023.

learning data and a robust system for preventing or correcting errors and biases";
- the public must be informed of the use of algorithmic CCTV.

Although these safeguards meet some of the LED requirements, there remains **a significant doubt regarding the compatibility of algorithmic CCTV systems with the principles of necessity and proportionality, and therefore with the lawfulness criterion pursuant to Article 8 LED.**

In May 2024, just after the beginning of the initial experimentation period and despite the absence of evaluation at that time, the French government proposed to extend the experimentation of algorithmic video surveillance until 2027, in a legislative proposal aimed at strengthening transport security.[77] The provision was declared inconsistent with the French Constitution by the *Conseil constitutionnel* because of a procedural issue.[78] Finally, that experimentation was then extended until 31 December 2027 by the law on the 2030 Olympic Games (hereafter "Olympic Games Act II").[79] Also, in March 2026, the Interior Ministry proposed a new draft legislation[80] to extend algorithmic CCTV beyond what the Olympic Games Act II already offers, aiming for the deployment of algorithmic CCTV at a local level.

In a 2022 position paper, the CNIL pointed out that such systems may lead to a large-scale processing of personal data, including in some cases sensitive data, and pose significant risks to individual and collective freedoms by creating a feeling of widespread surveillance.[81] The French DPA further added that the risks brought by generalised surveillance are even more acute when applied to the public space where individuals exercise their rights and freedoms: freedom of movement, expression and assembly, right to demonstrate, freedom of conscience and worship, etc. Yet the impact assessment discards any infringement upon the right to privacy due to "the absence of facial recognition [which] ensures anonymity in public spaces [...] and the safeguards in place [which] ensure the neutrality of the tool", and does not mention any impacts on other rights.[82] This contradicts the CNIL's conclusion that "the capture and, now, analysis of images of individuals in these spaces undoubtedly poses risks to their fundamental rights and freedoms".[83]

The CNIL further noted that the necessity of processing must be demonstrated by assessing the existence of less intrusive means of achieving the intended purpose, as well as the usefulness and the operational performance of the system in relation to the objective pursued.[84] However, this requirement is absent from the impact assessment.[85]

After the CNIL declared that, aside from the scope of Article 10 of the 2023 French Olympic Games Act, algorithmic processing of images and videos captured from closed-circuit television (CCTV) is

---

[77] https://www.assemblee-nationale.fr/dyn/16/dossiers/DLR5L16N49176
[78] Cons. const., 24 April 2025, ECLI:FR:CC:2025:2025.878.DC.
[79] https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000053707299
[80] https://www.senat.fr/dossier-legislatif/pjl25-472.html
[81] CNIL, "Caméras dites « intelligentes » ou « augmentées » dans les espaces publics", July 2022, available here: https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf
[82] Free translation from the original French in the impact assessment, available here: https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/ei_art_39_2022/ei_-spox2233026l_cm_22.12.2022.pdf
[83] Free translation from the original French in the position paper.
[84] CNIL, "Caméras dites « intelligentes » ou « augmentées » dans les espaces publics", July 2022, available here: https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf
[85] The necessity of traditionnal CCTV is also questioned by most scientific studies assessing its usefulness. See, among others: Antoine Courmont and Jeanne Salion, "Comment la vidéosurveillance se développe-t-elle dans les villages ?", 19 November 2021, available here: https://linc.cnil.fr/comment-la-videosurveillance-se-developpe-t-elle-dans-les-villages
In 2020, France's Court of Auditors reported that no correlation had been established between CCTV systems and the level of crime committed in public places or crime clearance rates (see: Cour des comptes, "Les polices municipale", 20 October 2020, p. 70, available here: https://www.ccomptes.fr/fr/publications/les-polices-municipales

illegal in public space based on the lack of a legal basis in the French Law,[86] the *Conseil d'État* confirmed that position twice.[87]

First, the *Conseil d'État* heard a case in a summary proceedings about the scope of Article 10, concerning a surveillance software developed by the company Veesion that uses an algorithm to detect suspicious behaviour in footage from CCTV systems deployed in supermarkets. In its June 2024 decision, the *Conseil d'État* came to the expected conclusion that supermarket CCTV cameras were outside the scope of Article 10 of the Olympic Games Act, and that supermarkets could not therefore algorithmically process any footage acquired from those systems.[88]

Second, in a January 2026 judgment, the *Conseil d'Etat* ruled that algorithmic CCTV, used by the city of Nice, was illegal.[89]

The compliance of mass algorithmic surveillance with data protection law was also challenged in the context of deployment of audio monitoring systems in several cities in France. Such systems include the recording and algorithmic analysis of sounds emitted in a public area, which, if considered suspicious, may trigger an alert to law enforcement, enabling them to point CCTV cameras towards the area concerned. The CNIL halted a project in the city of Saint-Étienne in 2019 and another one in the city of Orléans in 2023 following a complaint issued by the NGO *La Quadrature du Net*.[90] In both cases, the CNIL pointed out the absence of a specific legal basis for such systems, whether experimental or not, thus contravening the lawfulness requirement of Article 8 of the LED. In 2024, the Administrative Court of Orléans confirmed[91] that the system—which specifically linked microphones installed in public spaces to CCTV cameras—was illegal because it did not meet the necessity requirement.[92]

The lack of legal basis is often used to litigate such algorithmic surveillance in public space in court: in both the *Orléans*[93] and *Veesion* cases, courts sanctioned the lack of legal basis. The *Conseil d'État* followed that trend in January 2026 by ruling that the algorithmic CCTV used by the city of Nice was illegal.[94]

However, the lack of legal basis is not the only ground used to litigate algorithmic surveillance in public space. In January 2025, the *tribunal administratif de Grenoble* (Administrative Court of Grenoble)[95] ruled that Briefcam, an algorithmic CCTV software used by a small town (among others), was unlawful due to lack of clear purpose and proportionality.[96]

---

[86] CNIL, "Les cameras « augmentés » ou algorithmiques dans l'espace public", 18 November 2024, available here: https://cnil.fr/fr/cameras-augmentees-espaces-publics
[87] JRCE, 21 June 2024, ECLI:FR:CEORD:2024:495153.20240621; CE, 30 January 2026, ECLI:FR:CECHR:2026:506370.20260130
[88] JRCE, 21 June 2024, ECLI:FR:CEORD:2024:495153.20240621.
[89] CE, 30 January 2026, ECLI:FR:CECHR:2026:506370.20260130.
[90] Available here: https://www.laquadrature.net/wp-content/uploads/sites/8/2023/09/Courrier_CNIL_20230927_cloture_plainte_ASA_Orleans_anon.pdf
[91] The author represented LQDN in this case.
[92] TA Orléans, 12 July 2024, n° 2104478, available here: https://www.laquadrature.net/wp-content/uploads/sites/8/2024/07/1140081635_2104478_12072024_anon.pdf
[93] TA Orléans, 12 July 2024, n° 2104478, available here: https://www.laquadrature.net/wp-content/uploads/sites/8/2024/07/1140081635_2104478_12072024_anon.pdf
[94] CE, 30 January 2026, ECLI:FR:CECHR:2026:506370.20260130
[95] The author represented LQDN in this case.
[96] TA Grenoble, 24 January 2025, n° 2105328, available here: https://www.laquadrature.net/wp-content/uploads/sites/8/2025/01/2105328_24012025.pdf
See the explanation of La Quadrature du Net: https://www.laquadrature.net/en/2025/01/31/justice-finally-finds-briefcam-unlawful/

Biometric data:

While there is no specific definition of biometric data for unique identification given by the French Act, the last paragraph of Article 2 of the French Act[97] provides that, except as otherwise provided, the definitions given by Article 4 of the GDPR apply within the scope of the Act. Since Article 4(14) GDPR[98] gives the same definition for biometric data for unique identification as Article 3(13) LED, that definition is thereby incorporated into the French Act.

Article 10§IV of the Olympic Games Act explicitly states that the data processing it authorises does not use "any biometric identification system, [does] not process any biometric data and [does] not involve any facial recognition techniques".[99] This Act lacks a specific definition of biometric identification systems, biometric data, and facial recognition techniques.

In its decision of 17 May 2023, the *Conseil constitutionnel* ruled that biometric data means data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person,[100] aligning its definition with that given by the GDPR and the LED. It thus ordered the regulatory authority to ensure that the predetermined events to be detected by the algorithms do not lead to the processing of such data or the use of such techniques, but it did not reject the provision.[101]

However, it can be argued that if the purpose of algorithmic CCTV is to detect suspicious or dangerous activity in public spaces, it necessarily captures and analyses physical and physiological features and behaviours of individuals present in these spaces, such as their body positions, movements, or appearance.[102] The aim of the system requires isolating detected individuals from the background, which, it could be argued, amounts to "unique identification". As established by the GDPR and the LED, and as interpreted by the European Data Protection Board, the ability to uniquely identify a person can be achieved on the basis of their looks or other specific elements that distinguish them from the rest of the crowd.[103]

As a result, the legal classification of biometric data processing is not limited to facial recognition but includes any analysis and categorisation of individuals based on their physical, physiological and behavioural characteristics, provided that the aim is to identify and distinguish them in an environment. Therefore, the provision in Article 10§IV of the Olympic Games Act likely contradicts the interpretation of biometric identification and data under EU law. Moreover, the *Conseil constitutionnel*'s requirement of non-processing of biometric data, if following the definition under EU law, seems almost impossible to implement in light of the aims pursued by the algorithmic surveillance system under Article 10, and reflected in the list of predetermined events.

Web data mining:

Web data mining techniques have been experimented in France as part of the fight against tax-related fraud. Although it would normally fall under the GDPR, the *Conseil d'État* placed such processing under the rules of the LED.

In its *Puškár* decision of 27 September 2017, the Court of Justice of the European Union (CJEU) ruled that when data are collected and used for the purpose of collecting taxes and combating tax fraud, it does not appear that the processing of those data has public security, defence, or State security

[97] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037822959
[98] "(...) personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person (...)"
[99] https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000047561989
[100] Cons. const., 17 May 2023, ECLI:FR:CC:2023:2023.850.DC, §. 42: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047562010/
[101] Ibid, §. 49
[102] Among the categories of events to be detected according to the implementing decree, at least 6 directly imply the capture and analysis of individuals' bodies.
[103] EDPB, Guidelines 3/2019 on processing of personal data through video devices, v. 2.0, Adopted on 29 January 2020, available here: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

purposes.[104] The Court noted that "even if it does not appear to be excluded that that data may be used in criminal proceedings which may be brought, in the event of an infringement in the field of taxation, against certain persons whose names are included in the contested list, the data at issue in the case in the main proceedings do not appear to have been collected for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law."[105]

Moreover, in its *Valsts ieņēmumu dienests* judgment of 24 February 2022, the CJEU found that, when a national tax authority asks an economic operator to forward it data relating to taxpayers for the purpose of collecting taxes and combating tax fraud, it did not appear that this tax authority should be considered a "competent authority" within the meaning of Article 3(7) of the LED. Therefore, such processing falls within the scope of the GDPR.[106]

Explicitly founding its reasoning on this case-law, the *Cour de cassation*, the French Civil and Criminal Supreme Court, likewise ruled in its own judgement of 1 July 2023 that processing carried out by tax authorities pursuing the purpose of carrying out searches and seizures on the premises of a commercial company fell within the scope of the GDPR.[107]

In contrast, in its decision of 22 July 2022,[108] the *Conseil d'État* ruled that expansive and complex data mining and processing efforts by tax authorities and customs agencies fell within the scope of the LED, and not the GDPR, since the purpose of the processing was exclusively the investigation of criminal offences. More precisely, it ruled that processing operations for functionally different purposes and undertaken in the two separate design and implementation phases of a novel collection scheme should be evaluated together only on the basis of their ultimate stated purpose.[109] In that sense, the *Conseil d'État* did not follow the CJEU jurisprudence on the delineation between the GDPR and LED scopes, and instead focused solely on the purpose of the processing.

Article 154 of the 2020 Finance Act allows tax authorities and customs agencies to carry out data mining on an experimental basis, in the form of automated processing of publicly available data collected from social media and e-commerce platforms' websites. The stated aim is to fight fiscal fraud and other tax-related criminal activity by detecting suspicious transactions and fraudulent activity. The experimentation began in 2021. The 2020 Finance Act is implemented by Decree n° 2021-148 of 11 February 2021, which divides the processing into two different phases: a design and learning phase, and an operational phase.

During the design and learning phase, a sample of companies, natural persons, or webpages is created in order to develop data collection and analysis tools. From this sample, related data on people's identities and the contents of the sites are collected (e.g. texts, images, photographs, sounds, videos, etc., related to professional activities). Sensitive and identity data are deleted within five days of collection. Finally, "markers" or "criteria of relevance" are defined, such as key-words, metrics, dates or locations, which are thought to be signs of the criminal offences being monitored, developing patterns against which collected data will eventually be compared.

During the operational phase, any data required for the "markers" and "criteria of relevance" (such as civil status, user identification, pseudonyms, postal addresses, telephone numbers, email addresses or URLs of users' other personal pages) may be collected; that is, any data that may potentially reveal tax-related criminal activity. For the investigation of customs-related offences, the processing includes the collection of a wide variety of data, such as pictures of goods sold, shipping data, webpage traffic data, and data about how long the account has been active and its patterns of activity on the sites under surveillance. The only content excluded are comments and other forms of interaction that may appear on users' social media pages, whose processing is prohibited by Article 2 of the implementing Decree.[110] Finally, the collected data is compared against the patterns that were established in the design and learning phase. Matches are then transmitted to agents who are responsible for investigation and control.

---

[104] CJEU, 27 September 2017, *Peter Puškár*, case n° C-73/16, §39.
[105] CJEU, 27 September 2017, *Peter Puškár*, case n° C-73/16, §40.
[106] CJEU, 24 February 2022, *Valsts ieņēmumu dienests*, case n° C-175/20, §§45-47.
[107] Com., 1 June 2023, n° 21-18.558, ECLI:FR:CCASS:2023:CO00385
[108] CE, 22 July 2022, ECLI:FR:CECHR:2022:451653.20220722
[109] CE, 22 July 2022, ECLI:FR:CECHR:2022:451653.20220722, §. 7.
[110] https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000043129915

In its decision n° 2019-796 DC of 27 December 2019, the *Conseil constitutionnel* correctly observed that by enabling the undifferentiated collection, aggregation, and analysis of such a significant volume of data from social media and e-commerce platforms, the provisions of the 2020 Finance Act **constituted an interference with the right to respect for private life even if the data were made publicly available by a data subject.** It found, furthermore, that since they may discourage or limit use of those services, the provisions also **constituted an interference with freedom of expression and communication.**[111]

However, the *Conseil constitutionnel* also ruled that for most of the tax offences this system was intended to detect, and in defining the conditions for its use, the legislature had **sufficiently subordinated the data mining and processing to adequate safeguards**, thus striking an appropriate balance between data subjects' rights and the government's objectives.[112] Those safeguards were as follows:

> - only content that is openly available and relates to the person who willfully disclosed that content may be collected;
>
> - sensitive data must be excluded, including facial recognition data and data unrelated to the tax offences being monitored;
>
> - sensitive data must be deleted within five days of their collection, and other data within 30 days if they cannot be used to establish that a tax offence has been committed;
>
> - data should be stored only when strictly necessary for the purpose of detecting if a tax offence has been committed; they should be stored for no longer than a year after the completion of the criminal, tax, or customs enforcement procedure for which they were used as evidence, and no criminal, tax, or customs enforcement procedure may be initiated solely on the basis of automated processing.

The *Conseil d'État* issued its own judgment on the Financial Act's implementing decree on 22 July 2022,[113] after the *Conseil constitutionnel*'s decision. The *Conseil d'État* also rejected the complaint against the Act, as the Act only allows for the collection of content that is openly available and that relates to the person who willfully disclosed that content on e-commerce and social media websites linking different parties with a view to selling a good, supplying a service, or exchanging or sharing content, goods or services. However, users' own data that is only accessible to them after logging into such websites may not be collected.

According to the 2024 evaluation report, from approximately one million advertisements for goods and services collected by the fiscal administration since 2021, 160 cases of undeclared activity have been identified, and seventeen tax audits have been launched.[114] The CNIL indicated its regret that the report submitted was not sufficiently detailed to enable it to assess the proportionality and efficiency of the system.[115] However, it considered that the safeguards provided are satisfactory and the data appear to be adequate, relevant and limited to what is strictly necessary for the purposes for which they are processed.[116] In 2024, a decree implementing the new Finance Act extended the experimentation project for two more years, the scope of data collection to content accessible on online platforms which require registration for access and metadata (dates, times and geolocation of the content collected), and the scope of offences searched.[117]

---

[111]Cons. const., 27 December 2019, ECLI:FR:CC:2019:2019.796.DC, §. 83.
[112] Cons. const., 27 December 2019, ECLI:FR:CC:2019:2019.796.DC, §. 93.
[113] CE, 22 July 2022, ECLI:FR:CECHR:2022:451653.20220722, §. 14.
[114]"Information report to Parliament and the CNIL on the social media trawling system. Final assessment of the experiment" by the Directorate-General of Public Finance, published on 15 December 2023 by *Le Monde*, available here: https://www.documentcloud.org/documents/24224741-rapport-dinformation-au-parlement-et-a-la-cnil-sur-le-dispositif-de-chalutage-des-reseaux-sociaux/?mode=text
[115] CNIL, 14 November 2024, n° 2024-081.
[116] Ibid.
[117] Decree n° 2024-1274 of 31 December 2024

Localised census surveys and travel restrictions:

As stated in the Introduction of this report, as one of its security measures for the Paris 2024 Olympic Games, the government established an "Olympic Games Pass", which created and made use of records identifying everyone living within an arbitrary security perimeter within the city. Residents and bystanders were required to show their passes before entering the perimeter. The government's stated objectives were to prevent disturbances to law and order, and to maintain the security of major events, including the Games' opening ceremony. In its decision of 25 July 2024, the *Conseil d'État* ruled that these measures fell within the scope of the LED and not the GDPR.[118] The *Conseil d'État* therefore set aside objections based on the GDPR, without reviewing on its own motion the same objections based on the LED. The court ultimately upheld the data processing under the "Olympic Games Pass", ruling that its interference with the right to respect for private and family life, as guaranteed by Article 8 of the European Convention of Human Rights, remained proportionate to the legitimate aims pursued.

Intelligence agencies:

We lack information about the extent of big data analytic activities that may be authorised for intelligence purposes, as most of the regulatory acts relating to intelligence are not published.[119] The fact that any potential legal bases for such surveillance are not publicly available raises a serious concern about transparency and the potential for improper data collection and processing.

Predictive policing:

As part of a European initiative coordinated by the British NGO Fair Trials, LQDN published a report on the state of predictive policing in France.[120] It compiled the available data "on several predictive policing software systems formerly or currently in use within French police forces",[121] including:

> RTM (Risk Terrain Modelling), a "situational prevention" software program used by the Paris Police Prefecture to target intervention zones based on "environmental" data (presence of schools, shops, metro stations, etc.);
>
> PredPol, a software developed in 2015 within the government agency Etalab, tested in Val d'Oise in 2016 to assess the risk of car thefts, abandoned in 2017 or 2018;
>
> PAVED, a software developed from 2017 by the Gendarmerie and trialled from 2018 in various departments to assess the risk of car thefts or burglaries. In 2019, shortly before its planned nationwide rollout, the project was "paused";
>
> M-Pulse, previously named Big Data of Public Tranquility, developed by the city of Marseille in partnership with the company Engie Solutions to assess the suitability of municipal police deployments in urban public space;

[118] CE, 25 July 2024, ECLI:FR:CECHS:2024:495220.20240725, §§. 13-14.

[119] "Biometric recognition in public space: 30 proposals to avoid the risk of a surveillance society", information report n° 627, by Marc-Philippe Daubresse, Arnaud de Belenet and Jérôme Durain, members of the Senate, in the name of the Law Commission, filed on 10 May 2022, available here: https://www.senat.fr/rap/r21-627/r21-627.html

[120] https://www.laquadrature.net/en/2024/01/18/predictive-policing-in-france-against-opacity-and-discrimination-the-need-for-a-ban/

[121] https://www.laquadrature.net/en/2024/01/18/predictive-policing-in-france-against-opacity-and-discrimination-the-need-for-a-ban/

Smart Police,[122] an application that includes a "predictive" module and that is developed by French startup Edicia which, according to its website, has sold this software suite to over 350 municipal forces.[123]

LQDN concluded that these technologies conflate correlation with causation, use potentially discriminatory variables, are premised on false criminological doctrines, create serious risks of negative feedback loops and self-reinforcing effects, may enable abuses of power, and are of questionable efficacy. LQDN also notes that these technologies do not appear to meet the requirements of the GDPR and the LED since the secrecy surrounding their designs and implementation undermines data subjects' rights to effective remedies of abuses.

It is important to add that the use of these technologies is likely non-compliant with the LED requirements in the absence of a specific legal basis, in line with LED Article 8 on lawfulness of processing. Given the absence of a legal basis specifying the type and amount of data processed and the explicit and legitimate purposes of these systems, as well as the general lack of information available, it is impossible to assess their compliance with the requirements under LED Article 4, such as necessity, proportionality, accuracy, up-to-dateness, security, etc.

[122] The user manual of this software is available here: https://technopolice.fr/police-predictive/manuel-edicia/Presentation.html

[123] https://www.laquadrature.net/en/2024/01/18/predictive-policing-in-france-against-opacity-and-discrimination-the-need-for-a-ban/

Conclusion

In general, the French Data Protection Act closely mirrors the text of the LED. There are a few differences, however. For example, where Article 16(4) *in limine* of the LED requires that the controller must inform a data subject of any refusal to rectify or delete personal data, or to restrict its processing, and the reasons for the refusal, "in writing", Article 106§IV of the French Act does not specify "in writing". Variances such as this notwithstanding, the letter of the French law appears to faithfully transpose the text of the LED.

This does not, however, entail that France achieves full compliance with the LED. Administrative practices and case-law may, in some ways, fall short of the requirements of the LED, especially when combined with institutions' bad habits, institutional inertia and inadequate oversight mechanisms. This is notably the case with the lack of transparency of many administrative orders and their legal bases for data processing, which creates a substantial obstacle to ensuring effective judicial remedies.

French courts' very lenient interpretation of the "strict necessity" requirement is also cause for serious concern; it creates significant vulnerabilities to potential abuse and invites very large lapses in the government's compliance with the LED.

It is also likely a reality that despite significant increases over several years, the insufficiency of financial, human, and technical resources allocated to the CNIL adversely affects its investigations and handling of applications and complaints.[124]

As the first report of the European Commission on the application and function of the LED put it, "The LED has (...) been transposed in a satisfactory manner",[125] "but a number of outstanding issues remain".[126]

In order to improve the effective implementation and enforcement of the LED in France, the following actions appear necessary:

- urgently improve the respect of access, rectification, and erasure rights in relation to police databases, and implement the CNIL's recommendations in that regard;
- align the application of the requirement of "strict necessity" under Article 10 of the LED with the interpretation of the CJEU;
- align the interpretation of biometric data with the European Data Protection Board position and apply Article 10 of the LED requirement, notably that of "strict necessity", to algorithmic CCTV;
- increase the transparency and accessibility of administrative orders allowing data processing operations, for example by setting up a user-friendly, centralised platform;
- enforce stricter deadlines for administrative orders, making data processing operations by local and national authorities available to the public in due time to allow them to exercise their right to an effective remedy;
- increase the resources of the CNIL;
- cease the experimental and operational uses of technologies and data processing that do not comply with the principle of lawfulness under Article 8 of the LED and with Article 10 requirements, especially predictive policing and mass algorithmic surveillance systems;
- guarantee the regular, independent and evidence-based evaluation of data processing activities before the extension of their experimentation or implementation.

[124] https://www.statewatch.org/media/3823/11583-22.pdf p. 22.
[125] https://www.statewatch.org/media/3823/11583-22.pdf p. 35.
[126] https://www.statewatch.org/media/3823/11583-22.pdf p. 8.

Primary sources: Laws

French Data, Records and Freedoms Act of 6 January 1978 (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), available here:
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/2024-06-29/

Data Protection Act of 20 June 2018 (loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles), available here:
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952

Decree n° 2018-687 of 1 August 2018 implementing the French Data, Records and Freedoms Act of 6 January 1978 (décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles), available here:
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037277401

Decree n° 2019-536 of 29 May 2019 implementing the French Data, Records and Freedoms Act of 6 January 1978 (décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), available here:
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038528420

Finance Act of 28 December 2019 for 2020 (loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020), available here:
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039683923/2024-06-30/

Decree n° 2021-148 of 11 February 2021 on detailed rules for public finance services and customs services to carry out the mining by automatic processing of publicly available data on platform's websites (décret n° 2021-148 du 11 février 2021 portant modalités de mise en œuvre par la direction générale des finances publiques et la direction générale des douanes et droits indirects de traitements informatisés et automatisés permettant la collecte et l'exploitation de données rendues publiques sur les sites internet des opérateurs de plateforme en ligne), available here:
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043129895

2024 Olympic Games Act of 19 May 2023 (loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions), available here:
https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000046777392/

Decree n° 2024 -1274 of 31 December 2024 amending Decree No. 2021-148 of 11 February 2021 on the implementation by the Directorate-General of Public Finances and the Directorate-General of Customs and Indirect Taxes of computerised and automated processing enabling the collection and use of data made public on the websites of online platform operators, available here:
https://www.legifrance.gouv.fr/jorf/id/JORFARTI000050935033

2030 Olympic Games Act of 20 March 2026 (loi n° 2026-201 du 20 mars 2026 relative à l'organisation des jeux Olympiques et Paralympiques de 2030), available here:
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000053707088

Primary sources: Cases

Court of Justice of the European Union

CJEU, 19 March 2026, *Comdribus*, case n° C-371/24

CJEU, 26 January 2023, *Ministerstvo na vatreshnite raboti*, case n° C-205/21

CJEU, 24 February 2022, *Valsts ieņēmumu dienests*, case n° C-175/20

CJEU, 27 September 2017, *Peter Puškár*, case n° C-73/16

CJEU, 26 February 2013, *Åklagaren*, case n° C-617/10

European Court of Human Rights Case-law

ECtHR, 9 November 2006, *Sacilor-Lormines v. France*, n° 65411/01

CNIL

CNIL, 15 June 2023, deliberation n° 2023-068

CNIL, 17 October 2024, n° SAN-2024-017

Conseil constitutionnel (French Administrative Supreme Court) Case-law

Cons. const., 24 April 2025, ECLI:FR:CC:2025:2025.878.DC

Cons. const., 17 May 2023, *Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*, ECLI:FR:CC:2023:2023.850.DC

Cons. const., 27 December 2019, *Loi de finances pour 2020*, ECLI:FR:CC:2019:2019.796.DC

Conseil d'Etat (French Administrative Supreme Court, litigation section) Case-law

CE, 30 January 2026, ECLI:FR:CECHR:2026:506370.20260130

CE, 25 July 2024, ECLI:FR:CECHS:2024:495220.20240725

JRCE, 21 June 2024, *Veesion*, ECLI:FR:CEORD:2024:495153.20240621

JRCE, 4 January 2024, ECLI:FR:CEORD:2024:490447.20240104

CE, 20 December 2023, *Association Act Up Paris*, ECLI:FR:CECHR:2023:468295.20231220

JRCE, 21 December 2023, ECLI:FR:CEORD:2023:489990.20231221

JRCE, 12 December 2023, ECLI:FR:CEORD:2023:489923.20231212

JRCE, 24 May 2023, ECLI:FR:CEORD:2023:473547.20230524

JRCE, 6 May 2023, ECLI:FR:CEORD:2023:473716.20230506

CE, 22 July 2022, ECLI:FR:CECHR:2022:451653.20220722

CE, 26 April 2022, ECLI:FR:CECHS:2022:442364.20220426

CE, 24 February 2022, ECLI:FR:CECHS:2022:454424.20220224

CE, 30 December 2021, ECLI:FR:CECHR:2021:428028.20211230

CE, 24 December 2021, ECLI:FR:CECHR:2021:447518.20211224

CE, 24 December 2021, ECLI:FR:CECHR:2021:447515.20211224

CE, 24 December 2021, ECLI:FR:CECHR:2021:447513.20211224

CE, 21 December 2021, ECLI:FR:CECHS:2021:442360.20211221

CE, 24 September 2021, ECLI:FR:CECHR:2021:441317.20210924

CE, 29 July 2021, ECLI:FR:CECHS:2021:441621.20210729

CE, 22 July 2021, ECLI:FR:CECHS:2021:449461.20210722

CE, form. spéc., 12 July 2021, ECLI:FR:CEFSP:2021:426962.20210712

CE, 27 May 2021, ECLI:FR:CECHR:2021:441977.20210527

CE, Ass., 21 April 2021, ECLI:FR:CEASS:2021:393099.20210421

CE, 13 April 2021, ECLI:FR:CECHR:2021:439360.20210413

JRCE, 2 March 2021, ECLI:FR:CEORD:2021:449432.20210302

JRCE, 2 March 2021, ECLI:FR:CEORD:2021:449429.20210302

JRCE, 2 March 2021, ECLI:FR:CEORD:2021:447974.20210104

JRCE, 2 March 2021, ECLI:FR:CEORD:2021:447972.20210104

JRCE, 4 January 2021, ECLI:FR:CEORD:2021:447970.20210104

JRCE, 4 January 2021, ECLI:FR:CEORD:2021:447868.20210104

CE, 22 December 2020, ECLI:FR:CECHR:2020:446155.20201222

JRCE, 18 May 2020, ECLI:FR:CEORD:2020:440442.20200518

CE, Ass., 19 July 2019, ECLI:FR:CEASS:2019:424216.20190719

Conseil d'Etat (General Assembly, administrative section) Opinions

CE, AG (administrative section), 9 September 2021, opinion n° 403628

Cour de cassation (Civil and Criminal Supreme Court) Case-law

Crim., 4 April 2024, n° 23-84.530, ECLI:FR:CCASS:2024:CR00424

Com., 1 June 2023, n° 21-18.558, ECLI:FR:CCASS:2023:CO00385

Com., 11 October 2023, n° 22-15.070, ECLI:FR:CCASS:2023:CO00666

Cour administrative d'appel de Paris (Paris Administrative Court of Appeal) Case-law

CAA Paris, 25 April 2024, n° 22PA04404

CAA Paris, 25 April 2024, n° 22PA04271

CAA Paris, 7 February 2024, n° 22PA03387

CAA Paris, 7 February 2024, n° 22PA03408

CAA Paris, 13 December 2023, n° 22PA02827

CAA Paris, 14 June 2023, n° 21PA00637

Cour administrative d'appel de Lyon (Lyon Administrative Court of Appeal) Case-law

CAA Lyon, 23 March 2023, n° 21LY02015

Cour d'appel d'Aix-en-Provence (Aix-en-Provence Civil Court of Appeal)

CA Aix-en-Provence, 9 June 2022, n° 21/10364
CA Aix-en-Provence, 9 June 2022, n° 21/10368
CA Aix-en-Provence, 5 May 2022, n° 21/01443
CA Aix-en-Provence, 5 May 2022, n° 21/01446
CA Aix-en-Provence, 5 May 2022, n° 21/01445
CA Aix-en-Provence, 5 May 2022, n° 21/01449
CA Aix-en-Provence, 5 May 2022, n° 21/01444
CA Aix-en-Provence, 5 May 2022, n° 21/01441
CA Aix-en-Provence, 5 May 2022, n° 21/01448

Cour d'appel de Paris (Paris Civil Court of Appeal)

CA, 21 January 2022, n° 21/18573
CA Paris, 9 June 2021, n° 19/21343

Tribunal administratif de Bastia (Bastia Administrative Court)

TA Bastia, 15 February 2024, n° 2100495

Tribunal administratif de Caen (Caen Administrative Court)

JRTA Caen, 22 November 2023, n° 2303004

Tribunal administratif de Lille (Lille Administrative Court)

JRTA Lille, 29 November 2023, n° 2310103
JRTA Lille, 19 May 2023, n° 2304177

Tribunal administratif de Marseille (Marseille Administrative Court)

JRTA Marseille, 30 May 2023, n° 2304994
JRTA Marseille, 15 May 2023, n° 2304481

Tribunal administratif de Montpellier (Montpellier Administrative Court)

JRTA Montpellier, 13 October 2023, n° 2305795

Tribunal administratif de Nice (Nice Administrative Court)

JRTA Nice, 9 January 2024, n° 2306317
JRTA Nice, 9 January 2024, n° 2306307

Tribunal administratif de Rennes (Rennes Administrative Court)

JRTA Rennes, 2 May 2024, n° 2402098

TA Rennes, 11 April 2024, n° 2106360
TA Rennes, 23 March 2023, n° 2000241

Tribunal administratif de Versailles (Versailles Administrative Court)

TA Versailles, 8 November 2022, n° 2101294

Tribunal administratif de Grenoble (Grenoble Administrative Court)

TA Grenoble, 24 janvier 2025, *M. Le Querrec et Association La Quadrature du Net*, n° 2105328

Tribunal administratif d'Orléans (Orléans Administrative Court)

TA Orléans, 12 July 2024, *Association La Quadrature du Net*, n° 2104478

Secondary sources

"'Predictive' Policing in France: Against Opacity and Discrimination, Why a Ban is Needed", January 2025, written by LQDN as part of a European initiative coordinated by British NGO Fair Trials,[127] available here:
https://www.laquadrature.net/wp-content/uploads/sites/8/2025/05/polpred050525.pdf

Technopolice Website: https://technopolice.fr

La Quadrature du Net Website: https://www.laquadrature.net

CNIL's 2023 annual report:
https://www.cnil.fr/sites/cnil/files/2024-05/cnil_44e_rapport_annuel_2023.pdf

CNIL's 2024 annual report: https://www.cnil.fr/sites/cnil/files/2025-04/rapport_annuel_2024.pdf

CNIL, "Caméras dites « intelligentes » ou « augmentées » dans les espaces publics", July 2022, available here: https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf

Cour des comptes, "Les polices municipales", 20 October 2020, p. 70, available here:
https://www.ccomptes.fr/fr/publications/les-polices-municipales

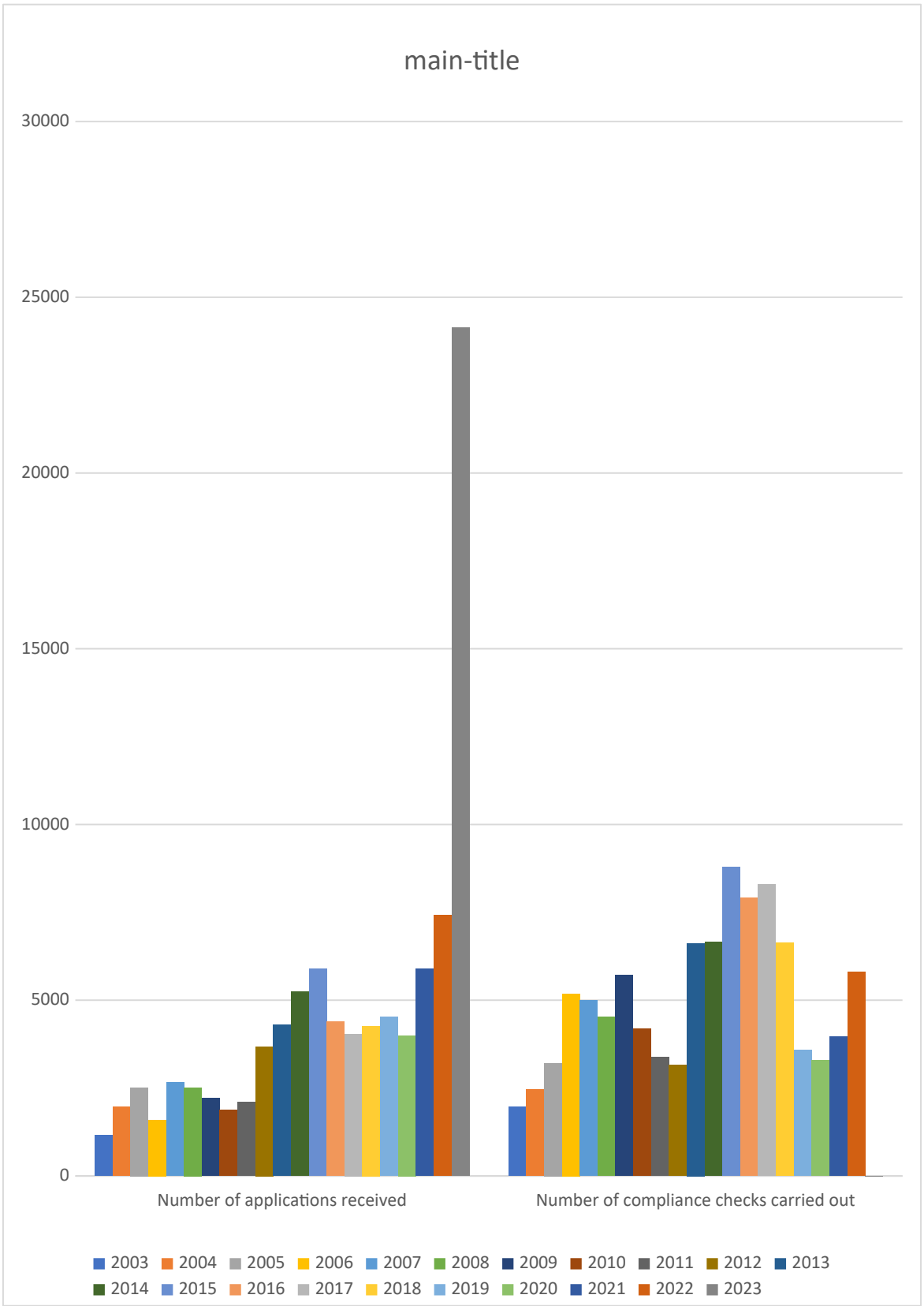
Antoine Courmont and Jeanne Salion, "*Comment la vidéosurveillance se développe-t-elle dans les villages ?*", 19 November 2021, available here: https://linc.cnil.fr/comment-la-videosurveillance-se-developpe-t-elle-dans-les-villages

Marc-Philippe Daubresse, Arnaud de Belenet and Jérôme Durain, members of the Parliament (Senate), "Biometric recognition in public space: 30 proposals to avoid the risk of a surveillance society", information report n° 627 in the name of the Law Commission, filed on 10 May 2022, available here:
https://www.senat.fr/rap/r21-627/r21-627.html

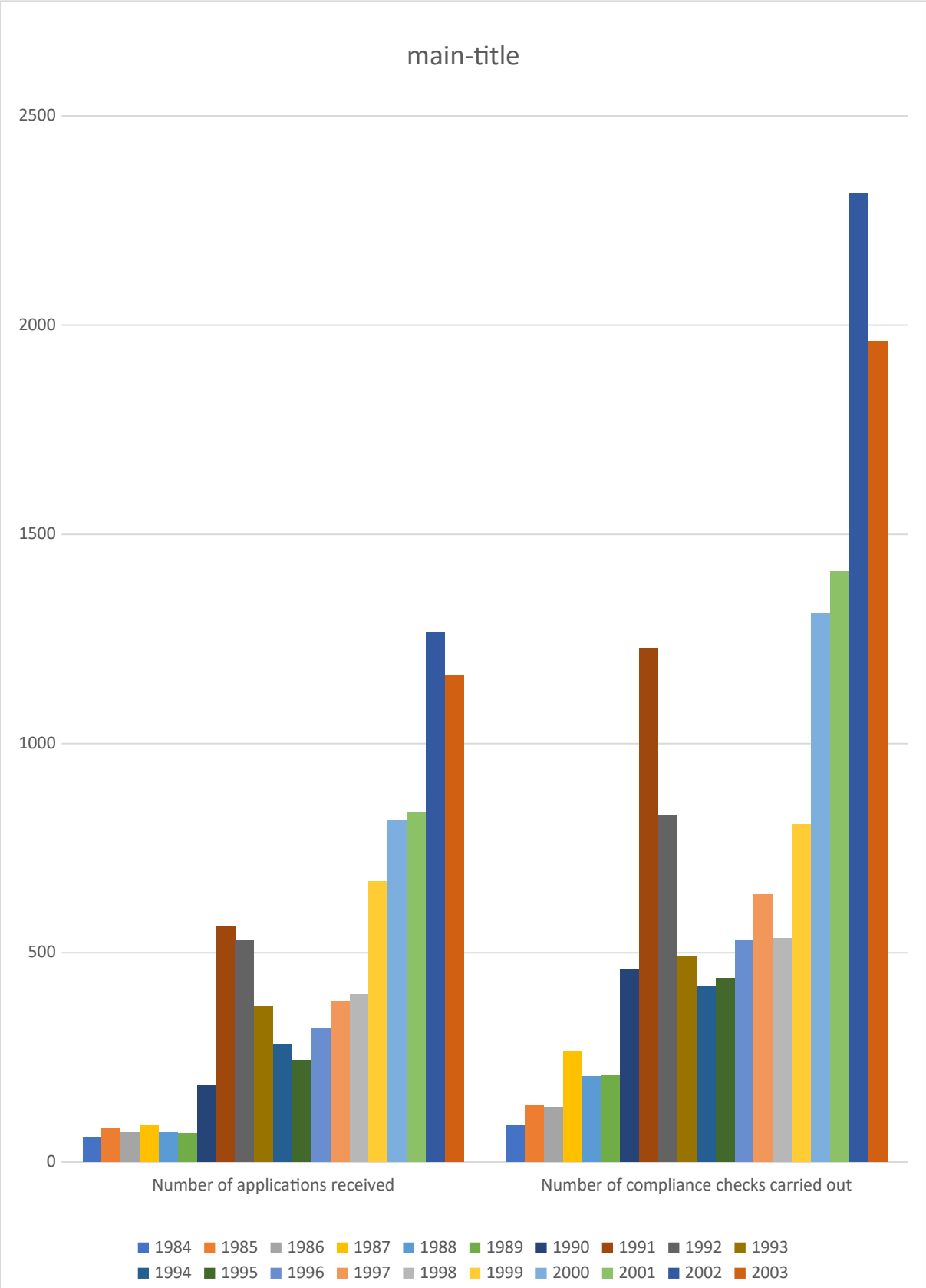
Philippe Gosselin and Philippe Latombe, members of the Parliament (*Assemblée nationale*), information report n° 1089 about the stakes of the use of security footage in the public domain for the purpose of fighting insecurity, filed on 12 April 2023, available here:
https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information#_Toc256000041

[127] https://www.fairtrials.org/

Annexes



Sources: https://www.data.gouv.fr/fr/datasets/exercice-des-droits-indirect-donnees-generales/ (Open Licence 1.0: https://www.etalab.gouv.fr/wp-content/uploads/2014/05/Licence_Ouverte.pdf); CNIL's 2023 annual report, p. 42



Sources: https://www.data.gouv.fr/fr/datasets/exercice-des-droits-indirect-donnees-generales/ (Open Licence 1.0: https://www.etalab.gouv.fr/wp-content/uploads/2014/05/Licence_Ouverte.pdf; CNIL's 2023 annual report, p. 42

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights