NEJVYŠŠÍ SPRAVNI SOUD

Seminar organized by Supreme Administrative Court of the Czech Republic and ACA-Europe

Supreme administrative courts and evolution of the right to publicity, privacy and information.

Brno, 18 May 2015

Answers to Questionnaire: France

Seminar co-funded by the "Justice" programme of the European Union

Supreme Administrative Courts and evolution of the right to publicity, privacy and information

(Questionnaire)

1. Briefly describe the administrative institutional backing of free access to information and of the protection of personal data. Whenever those agendas are institutionally linked, provide a brief description of such relations.

Response:

A) On access to information:

a) The right of access to administrative documents:

- In France, **Law no. 78-753 of July 17, 1978** grants every person **the right to obtain communication of documents held within the framework of its public service mission** by an administration, regardless of their form or medium.

Article 1 of the law of 17 July 1978 - which cites examples (non-exhaustive list) - gives a **very broad definition of administrative documents**: they refer to all the documents produced or received by the administration, whether they are presented in written form (records, reports, studies, minutes, statistics, directives, instructions, circulars, etc.), in the form of audio or visual recording or in digital or computerised form. This also includes information contained in computer files and information that can be retrieved by an automated processing tool in common use. In contrast, the following documents are not administrative: court documents, including financial and administrative courts, which are related to the judicial function; judicial documents relating to civil status; private documents; and documents of parliamentary assemblies[2].

This right is exercised in respect of all public entities **(the State, local authorities and their public institutions)** as well as in respect of **private bodies in charge of a public service mission.**

[1] **Law no. 78-753 of 17 July 1978 laying down various measures to improve relations between the administration and the public and various administrative, social and fiscal provisions.**

[2] Since the enactment of **law no. 2000-321 of 12 April 2000 relating to the rights of citizens in their relationship with the administrations**, all acts of parliamentary assemblies including acts governing the organisation and functioning of assembly departments are excluded from the scope of the law of 17 July 1978.

The law also provides for certain restrictions on the right to access, which are necessary to protect various secrets, for example those that guarantee respect for privacy or that guarantee in the interest of the public or that guarantee business confidentiality[3] in the interest of competition.

Every person has the right to request, without distinction of nationality or proof of standing, for the disclosure of an administrative document that does not call anyone into question. The administration referred to usually has one month to respond to a request[4], otherwise, the absence of a response is regarded as an implied decision to refuse the disclosure[5].

- After these deadlines**,** the matter can be referred to the **Commission for access to administrative documents - CAAD -** created by Article 20 of the aforementioned law of 17 July 1978.

This is an independent and advisory administrative authority responsible for monitoring freedom of access to administrative documents, as defined in Article 1 of this law. It has jurisdiction in matters of public archives (see response to question 4 for the system governing these archives) and re-use of public information (refer to b below). Under Article 21 of the same law, the Commission is also empowered to interpret the specific systems for communication prescribed by the texts listed in this article (for example, in medical, electoral, land registration and cadastral, association and other matters). These systems often introduce more liberal access which is however connected to the provisions of the general system of the law of 17 July 1978. In contrast, other provisions establishing specific access system exclude the application of this law (for example, access of an official to his records as part of a disciplinary proceeding, etc.). Consequently, challenging the refusal for disclosure opposed by the administrative authority on the basis of these special provisions cannot thus lead to a referral to the CAAD, but must be submitted directly to the territorial administrative court that has jurisdiction.

The composition of the CAAD guarantees its independence[6]. Its role is primarily to issue opinions on the refusal opposed by the administration to requests for disclosure submitted by individuals, companies or associations[7]. A matter must be referred to it before any appeal,

[3] **Article 6 of the Law of 17 July 1978**.

[4] There are exceptional arrangements that may provide for shorter periods: for example, for medical records less than 5 years old, the time period is 8 days and two months if the records are older than 5 years.

[5] **1st paragraph of Article 17 of Decree No. 2005-1755 of 30 December 2005 concerning the freedom of access to administrative documents and the reuse of public information, adopted for implementation of law no. 78-753 of 17 July 1978**).

[6] Under the terms of **Article 23 of Law No 78-753,** the Commission consists of eleven members: a member of the Council of State, a magistrate of the Court of Cassation and a magistrate of the Court of Auditors, a Member of Parliament and a Senator, an elected member of a local authority, a professor of higher education, a qualified person in the field of archives, a qualified person in the field of personal data protection, a qualified person in the field of competition and prices and a qualified person in the field of public dissemination of information.

[7] The activity of the CAAD in the last five years pertains to the review of about 5000 cases per year (advice and consultation combined).

subject to what has been previously indicated (for details of the proceedings, refer to the answer under 2.). It also advises administrations on the communicability of documents[8] and may be consulted by the Government or propose amendments to legislative or regulatory texts in order to promote the right of access and transparency. It informs the public about the right of access (especially via its website) and prepares an annual activity report, which is made public.

Furthermore, during the investigation of cases, useful exchanges have taken place between CAAD and officials of certain departments of ministries or large institutions. The CAAD wanted to expand this informal network so that its action is better relayed.

- In 2005, this intention was realised by the introduction of Article 24 of the Law of 17 July 1978 specifying the **appointment of persons responsible for access to administrative documents and questions regarding the reuse of public information.**

The bases of the network of the persons responsible referred to as "**PRAAD"** are laid down by the provisions of Title IV (Articles 42 to 44) of Decree No. 2005-1755 of 30 December 2005 concerning freedom of access to administrative documents and reuse public information[9] as well as Articles L. 124-3 and R. 124-2 of the Environment Code. The appointment must be made known to the citizens in accordance with the most appropriate procedures, such as publication on the website of the administration, if it has one.

The person responsible is in charge of accepting the requests for communication and any complaints, ensuring their examination and establishing a link between their administration and the CAAD. He may also be responsible for preparing an annual review of requests for access to administrative documents and licence for reuse of public information (for the latter point, refer to b). He thus plays a major role as regards difficulties encountered vis à vis access to administrative documents. He also fulfils the role of legal expert by advising his administration on the investigation of specific cases or by investigating them himself, if necessary, and by suggesting organisational improvements to facilitate access to documents communicable under the law.

[8] On issues for which the CAAD adopts a constant and well established response, consultation of the website (www.CADA.fr) provides information that gives the administration the opportunity to respond appropriately to requests for disclosure that are addressed to it.

[9] The network of persons responsible pertains to most of the entities that hold or create administrative documents, as defined in Article 1 of the law The following are required, under **Article 42 of Decree no. 2005-1755**, to appoint a person responsible: the ministers and prefects; the presidents of regional and general councils, the mayors of communes of over 10,000 inhabitants and the presidents of public institutions of inter-communal cooperation of over 10,000 inhabitants; the directors of national and local public institutions that employ at least 200 officers. The obligation extends to public law and private law entities responsible for the management of a public service, which employ at least 200 workers (hospitals, welfare offices, health insurance funds or pension funds, public offices for subsidised housing, tourist offices, etc.).

Finally, it should be noted that in case **of failure of the amicable phase before the CAAD, it is the exclusive responsibility of the administrative courts to hear disputes pertaining to the application by the administration of the law of 17 July 1978**[10]**,** as well as all the special systems for access to administrative documents (for details of the proceedings, refer to the response under question 2).

b) The reuse of public information:

- Before the entry into force of **ordinance no. 2005-650 of 6 June 2005**[11], Article 10 of the law of 17 July 1978 laid down a principle of prohibition of the reuse (including reproduction and dissemination) for commercial purposes of the documents disclosed under this law. The new provisions of Article 10 set out, however, **a principle of free reuse of public information,** under the reservations and the conditions provided for in **Chapter II of the law of 17 July 1978**.

All *"public* information" may be re-used *"by any person who wishes to obtain it for reasons other than those of the public service mission for the purposes of which the documents were prepared or received"*[12]. For a piece of information to be regarded as public, and to enter, as such, the scope of chapter II of the law of 17 July 1978, it must first be a part of an administrative document. Article 10, however, provides a series of exceptions. The following is not considered public information:

- **information contained in documents that are not subject to public dissemination or the communication of which is not a right for any person**[13]**:** on the contrary, the documents freely communicable on the basis of Article 2 of the law of 17 July 1978 or special systems (for example, derived from Articles L. 124-1 et seq. of the Environment Code, or Article L.2121-26 of the general code of local authorities, etc.) are in principle public information;

- **information contained in the documents prepared or received by the administrative authorities in the exercise of an industrial or commercial public service mission;**

[10] Refer to the decision of the Disputes Tribunal, 2 July 1984, Vinçot and Leborgne v/s Caisse MSA du Finistère, nos. 02324; 02325.

[11] **Ordinance no. 2005-650 of 6 June 2005 on freedom of access to administrative documents and the reuse of public information,** which transposes into domestic law the provisions of Directive 2003/98/EC of the European Parliament and of the Council on the reuse of public sector information.

[12] Thus, the reuse of public information includes the use by a journalist of public information contained in an administrative document (see CAAD, council No. 20074133 of 21 February 2008), such as the creation of graphic materials based on maps prepared by an administration (refer to CAAD, opinion no. 20060771 of 16 March 2006) or online uploading of administrative documents obtained under chapter I of Title I of the law of 17 July 1978 (refer to CAAD, consultation no. 20081565 of 17 April 2008).

[13] Refer to **CAAD, opinion no. 20060881 of 2 March 2006.**

- **the information contained in the documents on which third parties hold intellectual property rights**[14].

By derogation, the abovementioned Article 10 further provides that the exchange of public information between administrative authorities for the performance of their public service mission does not constitute a re-use.

If obtaining data entails a cost for the administration or if it wishes to obtain compensation for its intellectual property rights, it may require the payment of a fee after having concluded a reuse licence[15]. The non-compliance with the license terms or distortion of public information[16] is punishable - mainly by way of fines - imposed by CAAD, upon a complaint of the administration and under the terms of an adversary proceeding[17]. This is the only circumstance stipulated by the legislator under which the CAAD has a power of sanction[18].

B) <u>On the protection of personal data:</u>

In France, the right to protection of personal data is governed by numerous texts[19]. However**, law no. 78-17 of 6 January 1978 relating to data protection and privacy**[20], as amended by **the law of 6 August 2004**[21] **transposing the Directive 95/46/EC relating to the personal data protection**[22] remains **the fundamental text.** It sets the general framework applicable to the **protection of personal data in France** and defines the principles to be complied with for

---

[14] For aerial images, refer to **CAAD, consultation no. 20063777 of 14 September 2006**; for old photographs, **consultation no. 20071573 of 19 April 2007**.

[15] **Articles 15 and 16 of the law of 17 July 1978.**

[16] **Article 12 of the law of 17 July 1978**: "Unless otherwise agreed by the administration, the reuse of public information is subject to the condition that it is not altered, that their meaning is not distorted and that its sources and date of last update are mentioned".

[17] **Articles 18 and 22 of Law no. 78-753**. The procedures are specified **by Articles 20 to 26 of Decree No. 2005-1755 of 30 December 2005.**

[18] Such power is explained in the response to question 6 in B).

[19] Some articles of the Civil Code, the Penal Code or the Code on internal security as well as more than thirty laws, even if they deal with various elements, are related to the protection of personal data: for example, law No. 95-116 of 4 February 1995 concerning various social provisions; law no. 97-1159 of 19 December 1997 establishing electronic monitoring as a term of execution of custodial sentences; law no. 2002-303 of 4 March 2002 relating to the rights of patients and the quality of the system; law no. 2004-575 of 21 June 2004 relating to the confidence in the digital economy, etc.

[20] **Law no. 78-17 of 6 January 1978 relating to data protection and privacy**: *Official Gazette*, January 25 1978, p. 227.

[21] **Law no. 2004-801 of 6 August 2004 relating to the protection of individuals with regard to processing of personal data and amending law no. 78-17 of 6 January 1978 relating to data protection privacy**: *Official Gazette*, 7 August 2004 p. 14063.

[22] **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 relating to the protection of individuals with regard to the processing of personal data and to the free movement of such data**: *Official Journal of the European Communities*, no. L 281, 23 November 1995 p. 31.

collecting, processing and storage of personal data[23].

To ensure compliance with and implementation of the law of 6 January 1978 known as the "Data Protection" law, the legislators created an independent administrative authority**,** the **Commission nationale de l'informatique et des libertés (CNIL)** [National data protection authority]. The independence of the CNIL is guaranteed by its composition[24]. **With regard to the diversity of instruments** available to it to undertake the tasks assigned to it, the CNIL is a **regulatory authority for the protection of personal data[25]**

Thus, being in charge of monitoring compliance with the provisions of the law of 6 January 1978, the CNIL performs **highly varied tasks** that can be distinguished, **on the one hand**, between a priori **control** of processing operations[26] which results in the supervision of personal data protection sector and in the review of preliminary formalities to which all treatments prior to their effective implementation are subject, and **on the other hand**, a posteriori **control** of personal data processing operations in the context of complaints and recommendations received by the CNIL and its powers of control and sanction.

a) A priori **control exercised by the CNIL:**

- **The supervision of the personal data protection sector**.

- Advisory role. As the regulatory authority of the personal data protection sector, the **Commission nationale de l'informatique et des libertés is entrusted with a mission to provide consultation and guidance on actions** performed by different players[27]**.**

Firstly, as part of its advisory role, the CNIL **may** adopt **recommendations that** help set guidelines on the practical procedures for implementing the law on "data protection" in some

[23] **Article 1 of the law of 6 January 1978**establishes the principle according to which information technology is at the service of every citizen, that its development must take place within the framework of international cooperation while respecting privacy and individual or public freedoms. It applies both to public sector as well as private sector processing. Thus, the protection granted is independent of both the ownership of the data and its public or private nature.

[24] **Article 13 of the Law of 6 January 1978**. It comprises seventeen members from the highest courts, the Council of State, the Court of Cassation, the Court of Auditors, and parliamentarians, representatives of the Economic, Social and Environmental Council, qualified individuals, which guarantees pluralism and independence. It also includes a counsel for the defence of rights in an advisory capacity.

[25] The concept of "**personal data"** found in **Article 2 of the law of 6 January 1978** is interpreted broadly. It refers to any information that helps, directly or indirectly, identify a person in view of all the resources available to perform the identification in question. The rights and obligations associated with this protection are thus related to the identifying nature of the data.

[26] **Article 2 of the law of 6 January 1978**also adopts a broad definition of the concept of "**personal data processing**", since it refers to automated as well as non-automated processing i.e. a data file or a "paper" file containing personal information about individuals.

[27] Under **Article 11 para. 2, d) of the law of 6 January 1978,** the CNIL "responds to requests for opinions of public authorities and, where appropriate, the courts, and advises individuals and bodies that implement or plan to implement automated processing of personal data".

sectors[28]. It also gives **opinions** on the draft texts relating to the personal data protection. Finally, it helps in the **definition of the normative framework of personal data protection** by proposing, to the Government, legislative or regulatory measures on the adaptation of the protection of freedoms, and by providing **assistance to the other independent administrative authorities** to give its opinion on personal data protection.

- The **role of inspection of compliance of drafts with the law of 6 January 1978**[29]. The CNIL may give an **opinion on compliance** of draft professional rules, products, procedures, for the protection of individuals with regard to personal data processing.

- The **role of labelling. The CNIL has a jurisdiction in matters of labelling**[30] recognised products and procedures that comply with the law. The aim is to recognise and promote a high level of data protection at the request of professional organisations or institutions.

- The **supervisory role of the "data protection" (CIL) correspondents** created by the law of 6 August 2004[31] amending the law of 6 January 1978, and by the implementing decree no. 2005-1309 of 20 October 2005[32]. The appointment of such a correspondent allows the processing manager to reduce his obligations of declaration to the CNIL. He may refer a matter to the latter for difficulties encountered in the exercise of its duties after informing the personal data processing manager concerned[33].

- Task of provision of information. The CNIL performs a general task of provision of information to individuals and processing managers **about their rights and obligations[34].** The CNIL also presents each year **its annual report** which performs an assessment of its activity.

---

[28] Under the terms of **Article 11 of the law of 6 January 1978**, "For the fulfilment of its tasks, the committee may proceed by way of recommendation and take individual or regulatory decisions in the cases provided for by this law". See for example: CNIL, deliberation no. 2012-404, 15 November 2012, concerning recommendations relating to the processing of detailed consumption data collected by the communication meters.- CNIL, deliberation no. 2010-371, 21 October 2010, adopting a recommendation on the security of electronic voting systems.

[29] Article 11 para. 3° of the law of 6 January 1978.

[30] Article 11 para. 3° of the law of 6 January 1978.

[31] **Law no. 2004-801 of 6 August 2004 relating to the protection of individuals with regard to processing of personal data,** mentioned above.

[32] **Decree No. 2005-1309 of 20 October 2005 adopted for implementation of law no. 78-17 of 6 January 1978 relating to data protection and privacy**: Official Gazette, 22 October 2005 p. 16769.

[33] Article 22 para. 3 and 67 of the law of January 1978.

[34] Under the terms of **Article 11 para. 1 of the law of 6 January 1978**, the CNIL *"informs all concerned and all processing managers about their rights and obligations".*

- **Examination of the preliminary formalities**

Chapter IV of the law of 6 January 1978 provides that the implementation of personal data processing is possible only **provided that the preliminary formalities have been performed by the body or person in charge of this processing**. There is a gradation in the preliminary formalities depending on the purpose of the processing, its sensitivity in terms of type of data processed and the identity of its manager. The personal data processing operations are subject to either a **reporting system**[35] or to an **authorisation system**: prior authorisation of the Commission[36], authorisation by ministerial decree[37], or authorisation by Order of the Council of State[38] (see processing authorised by Order of the Council of State, see the response under question 3). The reporting system is a system of common law, the authorisation systems being reserved for categories of processing that pose special risks, such as those involving sensitive data or biometric data.

The bodies that have adopted a CIL are exempt from the reporting obligation.

b) A posteriori **control exercised by the CNIL:**

- The CNIL **exercises a posteriori control on the compliance of personal data processing, in the context of complaints and claims that it receives and its powers of control and sanction.**

It has jurisdiction to **hear the complaints of the persons concerned**[39] especially when they want to exercise their rights of access, rectification, erasure or objection. Thus, any person establishing his identity has the right to question the person responsible for processing personal data in order to obtain information relating to him which is being processed[40] and, where appropriate, request for correction or deletion of such information[41]. By way of derogation, Articles 41 and 42 of the law of 6 January 1978 instituted a right of indirect access with regard to processing involving State security, defence or public safety (for the terms of this derogation, see response under question 7)[42].

[35] Article 23 and 24 of the law of 6 January 1978.

[36] Article 25 of the law of 6 January 1978.

[37] Article 26. I of the law of 6 January 1978.

[38] Article 26. II and article 27 of the law of 6 January 1978.

[39] Article 11 para. 2° of the law of 6 January 1978.

[40] Article 39 of the law of 6 January 1978.

[41] Article 40 of the law of 6 January 1978.

[42] For these processing operations, a member of the CNIL from the higher courts is responsible for accessing, in the name and on behalf of the applicant, the information relating to him, in order to ensure that they comply with the conditions of legality.

- **The CNIL's power of control in the context of its task of inspection of the compliance of processing operations.**

Article 44 of the law of 6 January 1978 sets out the jurisdiction of the CNIL as regards control of personal data processing operations. This control must help either to **determine the existence of processing operations that have not been subject to such formalities** or to **ensure effective compliance of the declared or authorised operations with the law**. It is also within the scope of these same provisions that the control of the CCTV devices[43] by the CNIL is exercised.

- **The CNIL's power of sanction in the context of its task of ensuring compliance of processing operations.**

To ensure the compliance of the implementation of personal data processing with the provisions of the law of 6 January 1978, the CNIL has the power to compel bodies to fulfil their obligations.

The matter is referred to a limited bench of the CNIL with a request for sanction when **breaches of law** are identified after a control. The president of the CNIL **may serve a formal notice** to the processing manager to comply with the law of 6 January 1978.

If at the expiry of the period thus granted to ensure compliance, the processing manager has not taken the necessary steps, the president of the CNIL may refer the matter to a rapporteur to ask the limited bench impose a **sanction**. This may consist of a fine of up to €150,000[44] and/or, where appropriate, an injunction to stop the processing or withdrawal of the authorisation granted by the CNIL[45]. The penalty decision may be made public at the initiative of the limited bench[46].

C) The contact points between the right of access to administrative documents and the protection **of personal data:**

a) From a structural point of view, there is a point of junction between the CAAD and the CNIL through their respective compositions. Under the terms of Article 23 of law no. 78-53 of 17 July 1978, the CAAD comprises **a qualified person for the protection of personal data**, who is generally chosen from among the members of the CNIL.

b) From a material point of view, law no. 78-53 of 17 July 1978 directly or indirectly makes reference to law no. 78-17 of 6 January 1978, and *vice versa*.

[43] Article L. 253-2 and L. 253-3 of the Internal Security Code. As such, the CNIL has conducted more than 450 inspections in 2012, of which approximately one third concerned the video-protection devices.

[44] Article 47 of the law of 6 January 1978. This may be published on the website of the CNIL and in the Official Gazette or on the Légifrance website.

[45] Article 25 of the law of 6 January 1978.

[46] Article 46 of the law of 6 January 1978.

Firstly, **the law of 17 July 1978** provides that:

- **Regarding the communication of administrative documents,** in **its Article 6**:

"II.- The administrative documents (...) whose disclosure would undermine the protection of privacy may be communicated only to the person concerned."

- **Regarding the reuse of personal data,** it is possible only under certain conditions laid down by **Article 13 of the law**:

- On the one hand, it is necessary that the person to whom the data relates has given his **consent** or that **such data are anonymised,** unless a **legislative or regulatory provision** allows the reuse of such data;

- On the other hand, the second paragraph of Article 13 reiterates that the **re-use of personal data must comply with the requirements of the law of 6 January 1978**[47].

Secondly, **the law of 6 January 1978 ensures the conciliation of its own provisions with the right to communication of administrative documents, as governed by the law of 17 July 1978**, and thus provides, in its Article 37, that: *"The provisions of this law shall not prevent the application, for the benefit of third parties, of the provisions of Title I of law no. 78-753 of 17 July 1978 (...)./Therefore, the holder of a right of access to administrative documents or public records exercised in accordance with law no. 78-753 of 17 July 1978 cited above (...) cannot be regarded as an unauthorised third party within the meaning of Article 34".*

Before this provision[48], the Council of State considered that the right to communication of administrative documents established by the law of 17 July 1978 could not be exercised to the extent that the provisions of the law of 6 January 1978 were not applicable[49]. This led to the restriction of third party access along with the development of computerisation of the administration. Consequently, the CAAD, to which a request for access to personal information contained in a file or taken from automated processing was wrongly referred, had to forward that request to the CNIL[50]. Now, a third party can access information that, even if "personal" within the meaning of the law of 6 January 1978, is not covered by any of the secrets prescribed by the law of

[47] The Commission therefore recommended that a commune to object to the reuse of a DVD containing civil registration data that was inconsistent with the Heritage Code and the recommendations of the CNIL **(consultation no. 20065008 of 8 February 2007**).

[48] Introduced by **law no. 2000-321 of 12 April 2000 relating to the rights of citizens in their relations with the administrations in Article 29-1 of law no. 78-17, and then** introduced in its present form in **Article 37 of law 1978, by law no. 2004-801 of 6 August 2004 relating to the protection of individuals with regard to processing of personal data and amending law no. 78-17 of 6 January 1978 relating to data protection and privacy.**

[49] Refer to the **assembly decision of the Council of State (CS), 19 May 1985, Bertin, No. 40680**; **CS 15 February 1991, Paris Church of Scientology, No. 68639.**

[50] Refer to the **decision of the CS, 30 November 1984, Bertin, No.49166.**

17 July 1978, particularly because it does not concern private life or it does not carry any value judgment about an identified or identifiable individual.

2. 2. Describe in general terms the regular administrative and court procedure in a typical disputable case of free access to information. Also describe the procedural role of your supreme administrative court.

Response:

This response describes in detail the pre-litigation **(A)** and court **(B)** procedures that are available to any party concerned that was refused a disclosure of a document by an administration that it previously approached under the provisions of the law of 17 July 1978.

A) The recourse before the CAAD in case of refusal of disclosure of an administrative document:

Along with the administrative court, the CAAD plays a vital role when an applicant faces a refusal of disclosure that he intends to contest. The refusal of disclosure and its challenge are governed by Article 25 of the law of 1978 and by the Articles 17 to 19 of Decree No. 2005-1755 of 30 December 2005.

a) Referral to the CADA:

The 3rd paragraph of Article 20 of the law of 17 July 1978 provides that **the recourse before the CAAD is a mandatory prerequisite for any contentious appeal.** A contentious appeal introduced before the administrative court in the absence of recourse before the CAAD is therefore inadmissible[51]. This inadmissibility cannot be covered during the proceedings[52].

In principle, the matter must be referred to the CADA within a period of two months from the notification of the refusal or the tacit refusal (second paragraph of Article 17 of Decree No. 2005-1755 of 30 December 2005). However, the time periods are binding on the applicant only if the decision of refusal of disclosure was notified to him with the indication of procedures and deadlines for appeal (Article 25 of the law of 17 July 1978), including the obligation to first refer the matter to the Commission.

The request shall relate only to the refusal of disclosure. **The CAAD does not have any jurisdiction to rule on the legality of an administrative act or**

[51] On this point, refer to the decision of the CS**, 19 February 1982, Ms. Commaret, No. 24215**, which considers that "*it is clear from Articles 2 and 7 of the law of 17 July 1978 that when a request for disclosure of administrative documents has been rejected by express or implied decision of the administrative authority, that refusal cannot be referred directly to the court hearing a case of misuse of power. The applicant must have previously referred that refusal, within the period for bringing proceedings, to the Committee on Access to Administrative Documents*".

[52] On this point, refer to the decision of the CS**, 27 July. 1984 Gimbert, No.** 58137; including, even if the administration has itself referred to the CAAD a request for advice before the intervention of the refusal of disclosure: see the decision of the **EC, 21 September 1990, S.A.R.L. Villerupt Auto-Ecole, no. 89251.**

an administrative practice or to give a person an "interpretation of the law of 17 July 1978".

b) The procedure followed by the CADA:

The CADA acknowledges receipt of the request and shall immediately contact the administration designated by the applicant as the author of a refusal of disclosure, in order that he be sent the documents at issue and the reasons for refusal. **The authority questioned is required, within the period prescribed by the President of the Commission, to send the latter all useful information and documents and to give him the necessary assistance** (see on this point the response under the first question, A) a) relating to the person responsible for these questions, "PRAAD"). The members of the Commission and the rapporteurs appointed by the president may conduct an investigation necessary for the performance of their task.

The CAAD has, from the date of registration of the request by its secretariat, a period of one month to notify its opinion to the competent authority and the applicant (Article 19 of the Decree of 30 December 2005). However, failure to comply with the time limit does not affect the legality of the decision of refusal of disclosure.

The Commission refers the matter to the administration in question and the latter's response must be quick to be taken into account satisfactorily. This response must make it possible to distinguish cases where the lack of disclosure results only in a delay in the processing of the request, and those for which there is real interrogation as to whether it is possible to disclose the document requested.

The sessions of the CAAD - which is not a court and whose debate is not adversary - are not public. After a deliberation session, the opinion is notified to the applicant and the administration in the form of a single letter with the advice and the reasons.

c) The scope and follow-up action on the opinion of the CAAD:

Following its deliberations, the CADA issues a **favourable or unfavourable opinion** on the **total or partial** disclosure of the document. The citizen cannot expect the CAAD, even in case of a favourable opinion, to send the documents that he seeks[53].

The opinions of the CADA are **non-binding.** They do not constitute adversely affecting administrative decisions and are therefore not likely to be the

[53] Refer to the decision of the CS**, 25 May 1983, Holland, No. 33754.**

the subject of an appeal concerning misuse of power[54]. Only the administration's decision taken in view of the opinion is likely to be referred to the court hearing a case of misuse of power[55].

The administrative authority has one month from the receipt of the CAAD's opinion to make known the action it intends to take vis à vis the request (Article 19 of the Decree of 30 December 2005)[56]. The lack of response from the authority questioned for more than two months from the registration of the applicant's request by the Commission constitutes a confirmation of the refusal decision (even Article 19). No provision requires the administration to inform the applicant of its final position.

Depending on the year, 80-85% of favourable opinions of the CADA are followed by the disclosure of documents[57].

In case of persistent refusal of disclosure, the applicant may contest the decision before the administrative court.

B) The court procedure:

a) Refusal of disclosure and challenge before the administrative courts:

- Such disputes must be brought at first instance before the **Administrative Court** in whose jurisdiction the authority that made the decision of refusal has its seat.

✓ **The special conditions of admissibility of the appeals**

The applicant who has not received a satisfactory response from the CAAD can challenge before the administrative court the decision of refusal after two months from the date on which the Commission recorded its request for an opinion, regardless of the opinion. This starting point of the time period avoids any delaying tactic on the part of the administration.

In practice, foreclosures are quite rare and, the right of access being permanent, it is up to the applicant, on whom the time limit for contentious appeals is binding, to make a new request to the administration and follow the procedure again ensuring this time that the time limits are taken into account.

It should be noted that the applicant that requests the interim relief judge to order the disclosure of administrative documents pursuant to Article L. 521-3 of the Code of Administrative Justice is not required to first refer the matter to the CAAD[58].

[54] Refer to the decisions of the CS**, 27 April 1983, Époux Deplace, No. 34773**.

[55] Refer to the decision of the CS**, 27 April 1983, Zanone, No. 46476.**

[56] However, this abstention does not result in an administrative decision adversely affecting the applicant of the administrative documents: EC**, 19 March 1993, Garreau de Loubresse, no. 51035.**

[57] Refer to the activity reports on the CAAD website (www.cada.fr).

[58] See the decision of the CS**, 29 April 2002, Société Baggerbedrijf de Boer, no. 239466**.

✓ **Control and powers of the administrative court**

Under the terms of 4° of Article R. 222-13 of the Code of Administrative Justice, the president of the administrative tribunal or the magistrate designated for this purpose and fulfilling the minimum conditions of seniority gives a ruling at a public hearing after hearing the reporting judge.

The administrative courts review the legality of the refusal decision and thus indirectly evaluate the validity of CAAD's opinion. This is why there is a close coordination between the CADA and the administrative court.

The court has, in this particular context, **extended powers of investigation**. It may, by an interlocutory judgment, *"require the competent authorities to present all necessary documents"* to settle the *dispute,* including *"the documents whose refusal of disclosure is the very subject of the dispute"*[59], without it being necessary for the document to be communicated to the applicant[60].

The court may also make a visit to examine and operate a computer database, to assess whether it can be disclosed.[61]

This broad investigation power allows it to check whether the administration is entitled to check, in particular, whether it is a preliminary document, confidential document, protected document excluded from any disclosure (as defined in Article 6-I of the law of 17 July 1978) or a document with restricted communication (that is to say those that can be disclosed only to "the person concerned" under Article 6-II of the same law)[62].

It is also required to check the applicability of Article III-6 of this law, in its version resulting from the ordinance of 6 June 2005. The administration cannot refuse access to a document on the sole ground that it would include an indication covered by one of the secrets protected by law. These provisions also provide that: *"When the request concerns a document with indications that cannot be disclosed under this article but it is possible to conceal or to separate the indications, the document is communicated to the applicant after concealing or separating such indications."*

[59] See the **decision of the CS, 23 December 1988, Banque de France vs Huberschwiller, no. 95310.**

[60] See the **decision of the CS, 14 March 2003, Kerangueven, no. 231661.**

[61] See the **EC** decision, **SA Le Point vs SNCF, no. 304752:** the Council of State orders in an interlocutory ruling the disclosure by SNCF to the Council of State of the entire "CEZAR" database, if necessary by on site consultation, without these details being sent to the applicant.

[62] A document cannot normally, owing simply to its nature, be the subject of a refusal of disclosure on the basis of one of paragraphs of 2° of I of Article 6; therefore, it is still appropriate to examine whether, given the content of the requested documents, their disclosure actually risks infringing a confidentiality protected by I of this article (see **EC, 22 February 2013, Fédération chrétienne des témoins de Jehovah France, Nos 337987, 337988**).

The partial disclosure is subject to two conditions established by case law[63]:

- The document must be divisible, that is to say it must allow concealing details in practice (for example in case of an Appendix with names, or documents where the indications to be concealed relatively few);

- The concealment must not distort the meaning of the document or make the disclosure of non-beneficial.

Furthermore, to ensure the implementation of its decisions in a preventive manner, the court may order the administration, pursuant to Article L. 911-1 of the Code of Administrative Justice[64], to take enforcement action that necessarily implies its decisions, for example by requiring the administration to present the document in question to the applicant[65].

Finally, a non-suit decision is given when the document is officially published or disclosed after the action was brought[66].

When the urgency of the situation warrants it, it is possible to refer the matter to the administrative court in summary proceedings under Article L. 521-3 of the Code of Administrative Justice. The prior referral to the CADA is then not required[67].

- **The Council of State gives a final ruling as a court of cassation**:

Since the intervention of Decree no. 2013-730 of 13 August 2013, the judgment of the administrative court on the disputes relating to the consultation and communication of administrative documents or public records cannot be the subject of an appeal before the administrative court of appeal (2e of Article R. 811-1 of the Code of Administrative Justice). It can be challenged only before the Council of State, by way of an **appeal in cassation.**

Furthermore, on the occasion of such an appeal, the Council of State may be referred to by the applicant, if necessary, for a **priority preliminary ruling on constitutionality (PPRC),** on the basis of the first paragraph of Article 23 -5 of the ordinance of 7 November 1958 on the organic law on the Constitutional Council[68], allowing during the course of litigation the examination of the

[63] See the decision of the CS**, 4 January 1995, David, No. 117750.**

[64] Since the intervention of **law no. 95-125 of 8 February 1995**.

[65] Cases where it appears from the grounds of the court judgment that the administration was required to grant the applicant's request (see, for example, **EC 12 July 1995, Domarchi, No. 161803**, for the annulment of a refusal of disclosure of administrative documents on the grounds that these documents could be disclosed by right).

[66] See the decisions of the CS**, Section, 17 January 1986, MINEFI vs SA Dumons** and **EC, idem, MINEFI vs Société Chanel**.

[67] **CS 29 April 2002, Société Baggerbedrijf de Boer, no. 239466**.

[68] **Article 61-1 of the Constitution,** resulting from the constitutional reform of 23 July 2008 specifies that: "When, in the course of proceedings pending before a court, it is argued that a statutory provision infringes the rights and freedoms guaranteed by the Constitution, the matter can be referred to the Constitutional Council by the Council of State or Court of Cassation, which shall issue a ruling within a specified period."

conformity of a legislative provision in the Constitution[69]. According to the jurisprudence of the Council of State, the PPRC is referred to the Constitutional Council on the triple condition that the impugned provision is applicable to the dispute or to the proceedings, that it has not already been declared compliant with Constitution in the reasons and decision of the Constitutional Council, unless circumstances change, and that the question is new or of a serious nature.

Thus, for example, the Council of State refused to refer to the Constitutional Council the question of compliance with the rights and freedoms guaranteed by the Constitution of f) of 2° of I of Article 6 of law 78-753 of 17 July 1978, under which the documents whose consultation or communication would prejudice *"the execution of proceedings introduced before the courts or operations preliminary to such proceedings, unless authorized by the competent authority"* cannot be disclosed". In this case, the question raised, which was not new, was not of a serious nature[70] according to the Council.

b) The special case of compensatory remedy:

For the record - because such a remedy is considered uncommon[71] -, it is possible for an applicant to initiate a compensatory remedy before the administrative court in the event that the administration commits a fault in connection with the application of the provisions of the law of 17 July 1978 or special regimes for disclosure of documents.

The applicant must prove the existence of a direct and certain prejudice linked to such a fault. In the absence of prejudice, the Council of State has rejected the compensation for applicants who considered themselves victims of a forbearance or a delay, assuming them to be at fault, in disclosing the documents[72].

For example, it is because of "ill will" to provide documents on which the CAAD had ruled a decade ago that the State was ordered to redress the prejudice resulting from steps that the applicant was obliged to take to access the documents[73]. Without referring to any "ill-will", the

---

[69] The defendant may raise a PPRC for the first time in the first instance, but also as an appeal or in cassation. However, to be referred to the Constitutional Council, the PPRC must pass through a "double filter". First, the administrative court to which the matter is referred. Then, if necessary, the Council of State shall ensure, before the transmission of the PPRC to the Constitutional Council, that it meets certain conditions. The Council of State then filters the PPRCs sent by the administrative courts or raised directly before it. It has a period of three months to decide on the referral of the PPRC to the Constitutional Council. Otherwise, the matter is automatically referred to it.

[70] See the **decision of the CS, 26 December 2013, Société Les Laboratoires Servier, no. 372230.**

[71] Such conclusions do not have to be submitted beforehand to the CAAD and can be introduced directly before the administrative court. Most of the time, these are conclusions presented in a request where the findings for cancellation mainly request the cancellation of refusal of disclosure of a document by the administration.

[72] See the decisions of the **CS, 2 October 1987, Kahn, No. 70769**; **CS, 22 April 1992, ministre délégué chargé P&T vs. Toubol, No. 72718.**

[73] See the decision of the **CS, Sec., 10 July 1992, ministre de l'agriculture et Forêt vs. Touzan, no. 120047.**

administrative court may also condemn a public entity to pay compensation for damages caused by unlawful refusal of disclosure[74].

Finally, another hypothesis consists of the disclosure by the administration of a document in breach of Article 6 of the law of 17 July 1978, which also constitutes a culpable illegality and can cause prejudice to the person concerned (including moral prejudice resulting from damage to reputation) that must be redressed[75].

3. Describe the procedural role of your supreme administrative instance in the agenda of protection of personal data.

Response:

The Council of State has, for the protection of personal data, a **duality of function,** through the exercise of an **advisory mission (A)** and jurisdictional **powers (B)**.

A) The advisory role of the Council of State in creating automated processing of personal data:

Several personal data processing operations **may be authorised only by decree of the Council of State** after taking a reasoned opinion of the CNIL. This refers to **decrees of the Government for which the consultation of the Council of State is madecompulsory.** Following this consultation, the Government retains the choice between the provisions of its initial proposal and the changes proposed by the Council of State.

- Under the terms of Article 27-I of the law of 6 January 1978, the following must be authorized by decree of the Council of State:

- The processing of personal data carried out on behalf of the State, of a legal person established in the public interest or legal person established for a private interest, which relates to **data that also includes the registration number of the persons in the national identification directory for individuals** (Article 27, I, 1).

- The processing of personal data carried out on behalf of the State, which relate to **biometric data necessary for authentication or control of the identity of persons** (Article 27, I, 2). This category comprises the processing of data relating to foreign nationals not allowed on national territory falls under this category, in case of failure to meet the conditions for entry during a check at the border (FNAD[76]), the processing called OSCAR (tool for repatriation aid,

[74] See the decision of the **CS, 23 July 1993, no. 111364, min. Défense vs. Delaine, no. 111364**.

[75] See the decision of the **CS, 25 July 2008, Costa-Autrechy, app. no. 296505**.

[76] **CNIL, 18 January 2007, deliberation no. 2007-008**.

statistics and control) relating to foreign beneficiaries of the repatriation aid device funded by the French office for immigration and integration[77].

Article 27 has **more guarantees** than Article 26. Thus, when an automated processing has been established under the procedure of Article 27, *"the fact that one of its characteristics is mentioned in Article 26 is in any event irrelevant to the legality of its creation"* [78].

- Under the terms of Article 26-II of the law of 6 January 1978, the following must be authorised by decree of the Council of State:

- the processing operations carried out on behalf of the State, **which benefit State security, defence, public security** or whose **purpose is the prevention, investigation, detection or prosecution of criminal offences or enforcement of criminal convictions or security measures** where these processing operations include data which show, directly or indirectly, racial or ethnic origins, political, religious or philosophical opinions or trade-union membership of an individual, or which relate to the health or sex life of the latter. (See for details on these files, the response to question 7).

- Under the terms of Article 69 of the law of 6 January 1978, the following are considered relevant:

- the processing operations carried out on behalf of the State, which benefit State security, defence, public security or whose purpose is the prevention, investigation, detection or prosecution of criminal offences or enforcement of criminal convictions or security measures where these operations include a transfer of personal data to a State that does not ensure an adequate level of protection of privacy and fundamental rights and freedoms of individuals with regard to the processing of which the data is the subject or may be the subject.

B) The jurisdiction of the Council of State in the field of protection of personal data:

- The action of the CNIL is **supervised by the Council of State**. Article R. 311-1 of the Code of Administrative Justice provides that the Council of State has jurisdiction, **in the first and last instance**, to hear appeals against decisions of the CNIL **taken under its control and regulation tasks**.

- However, the Council of State **does not have jurisdiction** to hear, in the first and last instance, appeals against decisions taken by the CNIL **in another capacity or to hear other disputes concerning it, particularly the compensatory disputes**[79].

[77] Decree no. 2009-1310 of 26 October 2009 concerning the creation of automated processing of personal data relating to foreign beneficiaries of the repatriation aid system managed by the French office for immigration and integration **- CNIL, 16 July 2009, deliberation no. 2009-468.**

[78] See the assembly decision of the CS, **26 October 2011, Association pour la promotion de l'image and a., no. 317827.**

[79] **CS, 18 December 2013, Ms. Longo-Ciprelli, No. 365844.**

Thus, in its **decision of 7 January 2015**[80], the Council of State thus rules that "the request by which M.C. requests that the State be ordered, for the faults committed by the CNIL, which is one of the main authorities mentioned in 4° of Article R. 311-1 of the Code of Administrative Justice, to pay it an indemnity for damages that it claims to have suffered, is not directed against a decision taken by the CNIL bodies under the control or regulation tasks entrusted to this authority but raises a dispute of another kind concerning this authority". This is a dispute **of another kind relating to this authority under the jurisdiction of ordinary and administrative courts.**

Similarly, the refusal of access to data from a file opposed by the CNIL comes under the jurisdiction of the administrative tribunal. When the manager of a processing operation pertaining to State security, defence or public safety precludes **a refusal to indirect access or correction**, the indication thus provided to the applicant by the President of the CNIL cannot be regarded as the exercise by the CNIL of one of its jurisdictional tasks, but the **mere notification of a decision of refusal of access taken by the processing manager**. This decision, in case of dispute, **comes under the jurisdiction of the administrative tribunal** in whose jurisdiction the authority that has taken this decision has its seat[81].

- Note that, the applicant - like what has been stated concerning the right of access to administrative documents - can have recourse to the provisions of **Article 61-1 of the Constitution,** that is to say, a **PPRC** (see the response under the question 2, B) b)).

It is for this reason, for example, that **the Council of State, by a judgment dated 26 March 2012, Société Pages Jaunes Groupe**[82]**, refused to refer to the Constitutional Council a PPRC** pertaining to CNIL's sanctioning powers after the intervention of law no. 2011-334 of 29 March 2011 relating to the counsel for the defence of rights for *"securing the CNIL's action in the exercise of its powers to sanction, by making a clear distinction between prosecutorial, investigational and sanction functions"*. According to the High Court, the new provisions relating to the sanctioning power of the CNIL "*ensure separation of investigative functions from the those pertaining to sanctions within the CNIL*", because they prevent "*the members of the CNIL which that may have had to hear the breaches likely to be the subject of general powers of investigation and control [...] from sitting as part of the limited bench"*, in charge of issuing sanctions. Thus, the Council of State said that the question raised was, in this case, neither new nor of serious nature.

[80] **CS 7 January 2015, Catsiapis, no. 372328.**

[81] **CS 3 June 2013, Mr. Roxman, no. 328634.**

[82] See the **decision of the CS, 26 March 2012, Société Pages jaunes groupe, no. 353193**.

4. Provide for a general overview of historical development of access to information rights in your jurisdiction while focusing on most important legislative and judicial milestones. Also, please try to generally describe the main driving forces behind the development of these rights.

Response:

In France, the idea that the action of the administration must be known to the public is not new; Article 15 of the Declaration of human and citizen rights of 26 August 1789 provides that: *"Society has the right to call for an account of his administration from every public agent"*.

At the end of the nineteenth century, several laws provided for publication measures, in particular by way of display, for administrative decisions.

However, according to settled case-law formulated in the mid-twentieth century, the disclosure of documents held by the administration is a right only if provided by a text[83]. In the absence of a text prescribing and regulating the disclosure, the case law has admitted that nothing prohibited the administration to do so, since it did not infringe a legally protected right grant to third parties[84]. This case law was part of the tradition of secrecy that the administration liked to take support from and against which certain reforms intended to react as a result.

The citizens' claim of a right of access to administrative documents dates back to the 1960s with three arguments: the public, better educated, have the "right to know"; the administration, criticised for its taste for secrecy, is likely to benefit as this improves its image owing to the disclosure of records; the access to information held by the administration is a means of getting the opinion to support collective projects.

Being referred a draft bill that sought to improve relations between the administration and the public, the National Assembly changed the text **which became Title I of the law of 17 July 1978 titled "freedom of access to administrative documents"**. Also note the contemporaneity with the "CNIL" law (6 January 1978) and the law on archives (3 January 1979 - described below).

The number of beneficiaries of the right to information is unlimited since the law refers to *"any person*". Initially, the text adopted by the National Assembly attributed the benefit of the right of access to "citizens". The Senate judged this definition as too narrow since it excluded foreigners and legal persons, specially associations, when they are as concerned as nationals or individuals with the administrative "production". Also, the bill passed replaced the term "citoyens" (citizens) with the term "*administrés" (subjects).* But this improvement left some

[83] See the decision of the **CS, 18 Nov. 1949, Carlier: Rec. CS 1949, p. 490; CS, 12 March 1954, Gauthier: Rec. CS 1954, tables, p. 821.**

[84] See the decision of the **CS, 24 July 1981, Cadon, no. 24873.**

ambiguity with regard to the position of public officials. The law of 11 July 1979 amended the law of 17 July 1978 by replacing "administrés" (subjects) with the expression "*toute personne" (any person)*.

Undoubtedly, this law, which responds to a major contemporary need for transparency, marked a turning point in the conception of relations between administrations and citizens. It now forms the cornerstone of administrative transparency, around which many access systems for individuals revolve, which the CADA also adheres to since the order of 6 June 2005[85]. The amendments that were made to it by the law of 12 April 2000[86], and then by this order, has significantly helped endorse the doctrine that the commission has patiently developed, while always striving to maintain the balance between transparency to which citizens can legitimately aspire and the need to ensure confidentiality of certain information that these citizens themselves entrust the administration with and that pertains to their privacy or industrial and commercial confidentiality, or sensitive information concerning sovereign activities of the State.

With these developments, the right of access to administrative documents now consists of a **fundamental guarantee granted to citizens for the exercise of civil liberties** within the meaning of Article 34 of the Constitution[87]. As a result, only a law (not a decree or any other regulatory text) can regulate it.

The law of 17 July 1978 has undergone a major overhaul in 2005. The directive 2003/98/EC of 17 November 2003 on the reuse of public sector information has been transposed completely in French law by the order of 6 June 2005 cited above and decree no. 2005-1755 of 30 December 2005[88].

The order, which is inserted into the 1978 law, introduced, as the main innovation, the possibility of reuse of public information, hitherto excluded by law. It set out the principles and provides, in particular, power to impose penalties to the CAAD (see on this point, the response to question 6), which is recognised as an independent administrative authority already accepted by the Council of State. The decree of 30 December 2005 adopted for the application of the order replaces the previous texts. Another important amendment introduced by the 2005 texts concerns the appointment by the administrations of a person responsible for access to documents and reuse (see on this point, the response to Question 1, A) a)).

[85] **Ordinance no. 2005-650 of 6 June 2005,** cited above.

[86] **Law no. 2000-321 of 12 April 2000 relating to the rights of citizens in their relations with the administrations**, cited above.

[87] Refer to the decision of the CS**, 29 April 2002, Ilmann, no. 228830.**

[88] **Decree No. 2005-1755 of 30 December 2005 concerning the freedom of access to administrative documents and the reuse of public information, adopted for implementation of law no.78-753 of 17 July 1978, cited above.**

Other new provisions have been introduced in the domain of environment for transposing a directive 2003/4/EC of 28 January 2003 on public access to environmental information. The new wording of the Environmental Code taken from the law of 2 October 2005 and the decree of 22 May 2006 now provides for the application of the 1978 law, subject to special provisions[89].

Furthermore, it is also important to mention in the domain of **access to public information, the special system for public records**, which also underwent significant amendments and is associated with the system under the law of 17 July 1978. The system of archives was set by two major texts of the revolutionary period, the decree of 7 September 1790 and especially the law of 7 Messidor 1794. This law had proclaimed free access to documents contained in the filings, without any charge, conditions or restrictions. This was followed by texts, which were mostly originally regulatory, that restricted disclosure of archival documents and subjugated it to conditions. The law no. 79-18 of 3 January 1979 (for then on included in Articles L. 221-1 et seq. of the Heritage Code) restored order in this patchwork.

A renovation of this law was implemented by law no. 2008-696 of 15 July 2008 relative to archives. It strengthens the protection of public archives and undertakes to manage the public archives of local government groups and those of politicians[90], territorial authorities, institutions and public companies. The law[91] creates a new definition of archives, influenced by the new forms that technological advances have given to documents[92].

The transfer to archives does not result in the impossibility of disclosing the documents that were available earlier and at all times[93]. As a result, the documents that could be freely disclosed before being filed in the public records can still be disclosed without any restriction to any person who requests[94]

[89] Refer to **Article L.124-4 of the Environmental Code:** "After assessing the benefits of disclosure, the public authority may reject the request for information relating to the environment which upon consultation or disclosure may affect: /1 the benefits mentioned in Article 6 of law No. 78-753 of 17 July 1978 cited above, with the exception of those referred to in e and h of 2° of I of this article; (...)"

[90] Before this reform, the personal archives of a Member of Parliament, including correspondence with a prefect, were not regarded as public records in that they are not a product of the State's activity.

[91] See **Heritage Code, art. L. 211-1.**

[92] The archives consist of all the documents, irrespective of their date, form and physical medium, produced or received by any legal or physical person, and by any public or private department or body, for the purpose of executing their activity.

[93] See **law no. 78-753, 17 July 1978, Art. 2 paragraph. 3.**

[94] See **Heritage Code, art. L. 213-1, para. 1.**

for them and the administrative documents covered by the law of 17 July 1978 can still be disclosed under the conditions set out by this law[95].

The law makes the consultation of other documents in the public records subject to the passage of a time period. The reform of 2008 has lowered all these time periods particularly to meet certain expectations of civil society, especially those of journalists and academics who wish to further their investigative work or research. Thus, the general time period is now 25 years (reduced in 2008 from 30 to 25 years) in addition to the special time periods, which range from 50[96] to 100 years[97], instead of 60 to 150 years.

Finally, in respect of recent developments in the right of access to information, it is important to note the disclosure of public data or "open data", which is the subject since 2011 of a proactive policy of the Government, through the design of a unique inter-ministerial portal bringing together public information (see for further details on this point, see the response to question 5). The new challenge for the right of access to information is thus the effectiveness of this right through the provision of information to the public, without the public having to make a request to that effect.

5. Give basic subjective observation as to the role and importance of free access to information in political system of your country. In particular, focus on how the importance of freedom of information is perceived by general public and by nongovernmental sector.

Response:

The institutional mechanism implemented for access to public information - as described in the responses to questions 1 and 2 - and the recent changes thereto - as they are reported in the response to question 4 - show that the rule of law requires that administrative documents be accessible while respecting the necessary secrets, and that restrictions may be accepted and understood by all, even within liberal democracies. In France, **administrative secrecy has thus become an exception to the principle of the right of access to administrative document** on request made to any administrative authority that holds it. Since the order of 6 June 2005, this right of access to administrative document is coupled with a right to reuse the information that it contains, also established as a principle.

[95] See **Heritage Code, art. L. 213-1, para. 2.**

[96] in particular, the documents that contain information involving the protection of privacy or concerning State security or national defence (restrictive criteria) and appearing on a list established by a decree of the Council of State (decree. No. 79-1038 of 3 December 1979).

[97] in particular "the documents covered or having been covered by the confidentiality of national defence, the disclosure of which is likely to endanger the safety of named or easily identifiable persons", and the "documents relating to investigations carried out by the departments of the judicial police, to cases brought before the courts, subject to the special provisions concerning judgments, and to the execution of court decisions, the disclosure of which violates the privacy of the sex life of individuals" (Heritage Code, art. L. 213-2, I, 5°).

- **The mechanism for protection of the right to access** - described in detail in the response to question 2 - **is used most often with caution by the citizens and demonstrates all its effectiveness**. The total number of cases recorded by the CAAD in 2013 is 5486, including requests for opinions, advice and sanctions. By themselves, the requests for opinions made by those people who are opposed to a refusal of disclosure of administrative documents or public records amount to 5306[98]. 23% of opinions given were declared as not applicable in 2013, corresponding to a fulfilment of the request for access between the referral and the opinion of the CAAD. The effectiveness of mandatory preliminary remedy is widely demonstrated by this figure.

While **the number of cases before the CAAD is large, it remains in fact low** in view of the considerable volume of requests for access made daily to the administrative authorities. In addition, a part of the refusal of disclosure is due to the prudence of the administration, which prefers not to take the risk of disclosing information protected by secrecy and wait until the Commission decides on further action. Some authorities still ignore or do not consider the possibility of partially disclosing the documents, by concealing the information that is not to be disclosed. 49% of opinions in favour of the disclosure are given with reservations pertaining to the application of Article 6 of the Law of 17 July 1978, which means that the requested documents cannot be fully disclosed and it is recommended to first conceal the indications that are strictly protected by the secrecy mentioned in this article.

In addition, 178 advices at the request of the administrations were given in 2013 compared to 180 in 2012. This low number, with advices representing only 3.2% of the cases in the year, does not mean that the administrations rarely consult the CAAD. It first of all reflects an evolution in the processing of requests from administrations over several years. The questions that cover topics on which the Commission has ruled are handled by the General Secretariat, which responds by sending opinions or advice previously given on the same subject. Then, other than the processing of cases, the questions addressed to the Commission by the administrations - less formally - represented 850 letters, some 1800 emails and two phone calls of three, i.e. about twenty consultations per day.

The referral for the opinion of the CAAD thus plays an effective filtering role of reducing the number of litigation cases brought before the administrative court.

- In France, in addition to protecting the right of access which is fully ensured both by an independent administrative authority and, if necessary, by the administrative courts, the current focus is on improving conditions for disclosing to the public, public information - thus, in principle, information considered reportable. Since 2011, a movement initiated to create a new right has gained momentum in our country: **the movement for disclosing public data ("open**

[98] All figures quoted are from the 2013 public report of the CAAD. Please note, the requests for access to archives - which are highly residual - have generated fewer cases in 2013, 49 compared to 92 in 2012.

data") under which public information is intended to be made available to the public that is to say information provided irrespective of any request to that effect. This refers to disclosing public information that comprises neither details protected by Article 6 of the Law of 17 July 1978 nor any personal data, that is to say it can be provided to any person even before a request has been formulated.

The policy of disclosure and reuse of public data is managed, under the authority of the Prime Minister, by the **Etalab** mission, which continues the free provision of public data, in accordance with the general principle of free and easy reuse laid down by the **circulars of the Prime Minister of 26 May 2011**[99] **and of 13 September 2013 relating to the disclosure of public data**[100], by focusing on data with strong societal impact (health, education, etc.) and/or strong potential for economic and social innovation.

The mission works closely with the departments responsible for the modernisation of public action, including those responsible for innovation of the service provided to users and the digital transformation of the State, and has allowed the **creation of the portal "data.gouv.fr"**[101], cited above. The provision of public information by administrations meets their dual obligation of disclosing the administrative documents requested of them and allowing their reuse, subject to the reservation of protected secrets. In addition, the open data also meets an economic objective through the development of the digital economy which has major effects in terms of both growth and jobs as well as competitiveness and access to information.

The "data.gouv.fr" portal, which offers online services to enhance the transparency of public life and public confidence in the institutions of the Republic, is being well received in the French society. This policy is also well received internationally.

On one hand, this portal, which lists open data and the re-use made of these data, provides many examples of associations reusing public data or contributing themselves to the production of general-purpose data. It is the first governmental open data portal in the world to be open to all contributions, as it accepts general-purpose data generated by companies or association groups.

Moreover, last July, the UN ranked France as 4th in the world in terms of digital administration (and 1st in Europe), particularly welcoming the progress made in terms of open data and the open source policy.

---

[99] **NOR Circular: PRMX1114652C of 26 May 2011** relating to the establishment of the one-stop portal for public information of the State "data.gouv.fr" through the "Etalab" mission and the application of the provisions governing the right of reuse of public information.

[100] Jean-Marc Ayrault, the Prime Minister, sent a circular announcing the publication of the "Vademecum on disclosure and sharing of public data" on the platform www.datagouv.fr. on 13 September 2013 to the members of the Government.

[101] This includes a total of **13,827 sets of data**, from all administrations and civil society, which are freely accessible and reusable on data.gouv.fr.

France moved from the 16th to 3rd spot worldwide in terms of open data, according to the *Open Knowledge Foundation* (OKFN), an independent international association created in 2004 to promote open data. The Open Data Index analyses each year the level of disclosure of public data in 97 countries, from the United Kingdom (1st) to Guinea (97th) to Japan (19th) and Switzerland (24th). France ascent in the rankings can be explained by the provision of LEGI bases (legislative texts) by the Directorate of Legal and Administrative Information (DILA), the implementation of open source licensing of certain data of the Institut national de l'information géographique et forestière (IGN) [National institute for information on geography and forestry], or the provision of all election results at a single location, by the Ministry of Interior.

Recently, this institutional arrangement has been enriched with the mission assigned to **Chief Data Officer**, a position created in September 2014 by the Prime Minister[102]. He is responsible for stimulating the flow of quality data within the administration, and encouraging the administrations to make full use of these data by spreading the new practices of "data science" and big data within public departments.

The disclosure of data is the foundation of a movement towards the disclosure of decisions and informed participation of citizens in public decision-making. Elected to the steering committee of the **Open Government Partnership** in August, France is now taking an active part in this international community of governments and NGOs.

In this spirit, the Etalab mission conducts meetings and dialogues, particularly by means of an **extensive consultation process on digital technology entrusted to the CNNum[103]** (French Digital Council) by the Prime Minister, to define, in cooperation with civil society, and particularly the voluntary sector, a national action plan for open democracy, which will be presented to the Open Government Partnership. This action plan, oriented towards concrete decisions, will help boost transparency, citizen engagement, participation of all in public life and the informed contribution of citizens in public decision-making.

The display by the public authorities of a willingness for disclosure is primarily part of the instruments of "soft law". This is the case with the "**Vademecum on disclosure and sharing of public data" of 17 September 2013"**, sent by the Prime Minister to the ministers is an example. The vademecum provides that: *"All data produced or held by the administration which come within the scope of public data must be shared for free, and must be freely reusable"*. Internationally, France also contributed to the adoption of a soft law instrument, **"G8 Open Data Charter" of 18 June** 2013, which sets

[102] **Decree No. 2014-1050 of 16 September 2014 establishing a Chief Data Officer.**

[103] The National Digital Council is an independent advisory committee, whose tasks have been redefined and extended by decree of the President of the Republic of 13 December 2012. The National Digital Council's mission is to independently develop and publish opinions and recommendations on all matters relating to the impact of digital technology on society and the economy. To this end, it organises regular dialogues at the national and territorial level, with elected officials, civil society and the business world. It can be consulted by the Government on any draft law or regulation in the digital domain, as is the case here with the digital bill, currently being prepared and comprising, in particular, provisions on open data.

the principle of "disclosure by default"; in accordance with this Charter, it adopted on 6 November 2013 an action plan defining its priorities.

In its annual study in 2014 on the subject: *"Digital technology and fundamental rights",* the Council of State thus noted that *"the exhibition of a principle of disclosure by default is enshrined in a soft law instrument, in contrast to the weakness of the obligations under hard laws. The law of 17 July 1978 (...) does not provide for (...) the general obligation of online publication: its Article 7 requires the publication of only "the directives, instructions, circulars, and ministerial memos and responses which include an interpretation of the positive law or a description of administrative procedures"; for all other administrative documents, the publication is optional. (...)".* However, aware of the difficulties that can stimulate the inclusion of such a principle in the law, the Council of State advocates the path of soft law to promote the development of open data, particularly with regard to local authorities. The Council thus formulates under its proposals resulting from the aforementioned study to develop a charter of commitments and good practices by the State, associations of local authorities and representatives of data users (associations engaged in the disclosure of public data, and companies). This charter would ensure that each member public body defines a programme for disclosure of its public data, complies with quality standards and minimises the risk of re-identification.

Specifically, with regard to this last point, the criticism often made by citizens regarding open data consists of the possible invasion of privacy that such a disclosure information can entail. A large part of public data has no connection with personal data[104]. However, the administrations also manage a large number of databases relating to individuals[105]. The question of **compatibility between the policy of disclosure of public data and the protection of personal data** is thus likely to arise for each administration. The legislation has a clear answer for this in terms of principles. Article 7 of the law of 17 July 1978 states that the publication of data is subject to the implementation of processing that makes the identification of individuals "impossible". Article 13 authorises the reuse of public information containing personal data only if the person concerned has consented to it, if the authority holding the data is able to ensure that the data remains anonymous or it a legislative or regulatory provision so permits; the person re-using the data must in any event comply with the law of 6 January 1978. In practical terms, the question of what constitutes satisfactory anonymisation is rather more delicate; in the words of the G29 in an

[104] This is the case of the number of datasets presented as the "most popular" on the platform www.data.gouv.fr: the list of buildings protected as historical monuments, the "value added" indicators of schools for general or technological training, reporting charts for waste or observational data of the major weather stations.

[105] One of the most popular datasets on the site www.data.gouv.fr, the aid received by each beneficiary under the common agricultural policy (CAP), has also seen its legal basis partially invalidated by the CJEU for infringement of the right to protection of personal data: it ruled that regulations of the European Union that imposed the publication of the amounts received by each beneficiary were a disproportionate interference with this right, with regard to the aid received by individuals (CJEU, Gde Ch., 9 November 2010, Volcker and Markus Schecke GbR and Hartmut Eifert C-92/09 and C-93/09.

opinion of 10 April 2014, the "pseudonymisation" does not suffice to ensure "anonymisation"[106]. Efforts in this regard must therefore be pursued by the different administrations; the Council of State for example advocates, under its proposals for the above mentioned annual study, having anonymisation standards defined by the CNIL in consultation with the CAAD and constituting a centre for expertise in this area within each department.

6. Provide a subjective general observation as to whether and eventually how free access to information rights are in practice abused or misused by the petitioners.

Response:

A) As regards access to administrative documents:

- Firstly, to maintain the serenity of the action of the administration and limiting the constraints imposed on it by the right of access**, Article 2 of the law of 17 July 1978 does not oblige it to disclose documents that are**:

- **incomplete,** that is to say in preparation,

- **preliminary** to a decision as it is not taken, except as defined in paragraph 2 of Article 2[107],

- **publicly disseminated**.

In general, the law of 17 July 1978 does not compel the administration to reconstitute a document that has disappeared[108], to prepare documents that do not exist[109], for example, to respond to a request for information, or to conduct research to identify the documents requested. It concludes from this, like the administrative courts, that the law of 1978 *"does not aim to or result in requiring the relevant department to conduct research in order to provide the applicant with a document on a particular subject"*[110].

[106] Article 29 Working Party, "Opinion 05/2014 on Anonymisation Techniques", 10 April 2014, 0829/14/EN WP216.

[107] This refers to opinions, provided for by laws and regulations, in view of which a decision is taken on a request that tends to benefit from an individual decision creating rights, which can be disclosed to the author of this request.

[108] It seems that the law of 17 July 1978 is not expected to impose the transmission of a document that was lost and that could not be found despite extensive research **(CS, 11 Dec. 2006, min. Aff. étr. c/ Laurent, no. 279113**).

[109] The document is a material is that must physically exist at the time of the request for disclosure. It is obviously impossible to communicate an alleged document that does not exist or does not exist yet **(CS, 8 Jan. 1992, Synd. CFDT établissements et arsenaux Val-de-Marne, no. 74131**).

[110] See, on this point, the following decisions: **CS, 9 March 1983, Association SOS Défense**, **no. 43438**; **CS, 27 September 1985, Ordre des avocats au barreau de Lyon vs. Bertin, no. 56543**; **CS, 30 September 1987, Cie générale des eaux, aux tables, no.66573.**

- Secondly, **under the control of the CAAD and the administrative court,** the administrations are not required to respond to **requests that are grossly unreasonable** in terms of their volume or frequency and are formulated with the intention of hindering the activities of the departments[111].

According to the CAAD, a request is unreasonable when the evident purpose of the request **disrupts the functioning of the public department.** The Commission - like the administrative court, if a matter is referred to it - relies on a body of evidence[112] and decides on a case by case basis. The following criteria are taken into account: the number of requests and the volume of documents requested; the repetitive and systematic nature of the requests, particularly on the same subject[113]; the intention of putting the administration, in view of the volume, in a position that makes is physically impossible to process the requests; or the possibility that the applicant has or had to access the document in the recent past; the existence of a strained situation or even legal disputes between the applicant and the administration hearing the matter[114]; the latter's refusal to pay the expenses that have been requested.

In general, the Commission recommends the development of communication procedures that are compatible with the proper functioning of the administration, particularly by way of scheduled execution and the search for a negotiated solution between the applicant and the administration sought, rather than opposing the unreasonable nature of the request. In no case shall the administration resort to the notion of unreasonable request for "restricting" a priori the annual number of requests for disclosure made by the same person[115]. The unreasonable nature is evaluated from request to request, and not in consideration of the applicant himself. The latter cannot be denied, in general, his right of access. On the contrary, it is his responsibility to exercise this right with discretion.

The CAAD thus acts as a filter on which the administration can rely. If nevertheless it rules in favour of the applicant, the administration can persist in refusing to disclose the document. Thus, it will be up to the administrative court, to which the applicant referred the matter, to give a ruling (according to the procedure previously described under question 2, in B).

The administrative court also adopts an *in concreto* approach to the notion of "unreasonable request", since the provisions of Article 2 of the law of 1978 indicate only examples of

---

[111] **Article 2 of the law of 17 July 1978**expressly states that "the administration is not required to respond to unreasonable requests, particularly in terms of their volume, and their repetitive or systematic nature".

[112] Note that, according to the 2013 CAAD activity report, the proportion of its unfavourable opinions vis à vis the disclosure of documents given on the grounds that the request was unreasonable are 7% in 2009; 11.3% in 2010; 3.2% in 2011; 5.3% in 2012 and 1.94% in 2013 respectively.

[113] This criterion is also willingly accepted by the administrative court: see the decision of the **CS, 28 November 2014, M. et Mme de Keguelin, no. 373127.**

[114] Cf. **CAAD, opinion no. 20074652 of 6 December** 2007 for systematic requests for documents whose nature is wrongly identified, which the applicant himself prepared in part and which are requested in the context of a tense situation with the administration.

[115] On this point, refer to **CAAD, opinion no. 20090004 of 15 January 2009.**

reasons to qualify an unreasonable request and not the legal criteria that could substantiate this qualification. The unreasonable nature of a request results from the circumstances of the case that characterise it[116].

Therefore, it will take into account the possibility that the applicant has or had to access the document in the near past: cases where an applicant has already obtained a few months earlier, the records to which he has requested access; cases where the applicant produces, in support of his request to the Council of State, a copy of the documents that he has requested for disclosure[117].

However, the fact that the applicant may have obtained in the past, the disclosure of administrative documents, particularly in connection with proceedings before the courts, is not enough to legally justify the refusal to grant the request that the documents be communicated to him on the basis of the law of 17 July 1978[118].

- Finally, for the record, there will be **fines for unreasonable recourse** taken on the basis of the provisions of Article R. 741-12 of the Code of Administrative Justice. The administrative court may, in fact, impose on the author of a request that it considers unreasonable - and regardless of the subject of the dispute - a fine not exceeding 3000 euros. However, this is a specific power of the court, which is hardly used and the fines imposed rarely attain the maximum amount[119].

B) As regards the reuse of public information:

As has been stated in b) of A) in the response to Question 1, Article 18 of the law of 17 July 1978 entrusts the CAAD, following a complaint by the administration, a **sanctioning power,** i.e. when the reuse of public information has been made in disregard of the obligation to hold a license or license requirements; or when, unless approved by the administration, the public data have been altered or their meaning has been distorted.

The **penalties** are as follows:

- **in case of non-commercial reuse**, the Commission may impose a fine of **a maximum of 1500 euros**;
- **in case of commercial reuse**, the **fine,** is **proportionate** to the severity of the breach and the benefits derived from such breach and **may not exceed €150,000** (**€300,000 in the case of a repeat offence** within five years or **5% of the turnover excluding taxes** of the last financial year within this same limit);

[116] On this point, refer to the decision of the **CS, 25 July 2013, Commune de Sanary-Sur-Mer, no. 348669.**

[117] On this point, refer to the decision of the **CS, 8 January 1988, Van Overbeck, no. 50619.**

[118] On this point, refer to the decision of the **CS, 5 May 2008, Thiebeaux, no.294645**.

[119] For an example on the right of access to administrative documents, refer to: decision of the **CS, 5 May 2008, 21 May 1986, Bertin, no. 73271,** for a request that clearly does not fall within the jurisdiction of the administrative court (the amount imposed being 2000 F at the time, i.e. about 300 euros).

- **in all cases,** the Commission may, instead of or in addition to the fine, **prohibit the offender from re-using the public information** for a period of two years (five years for repeat offenders after the first infringement) and **order the publication of the sanction** at the offender's expense.

It must be noted that disputes concerning **reuse are quantitatively extremely low** and thus represent since 2010 less than 2% of all cases referred to the CAAD. Invested with this sanctioning power, the CAAD until 2013 had been referred a matter only once and had sanctioned in that case, the distortion of reused public information. In 2013, the CAAD has received two sanction requests from two communes; in both cases, the Commission decided that there was no need to impose a penalty.

7. Give a list and brief explanation of security, law enforcement and/or defence institutions that can benefit in your country from the exceptions laid down in Art. 7(e), Art. 8(4) and 8(5) of the Directive 95/46/EC.

Response:

First of all, the provisions of law no. 78-17 of 6 January 1978[120] introduce a derogation for files concerning State security, defence or public security as well as those whose purpose is the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sentences or security measures.

From a procedural standpoint, these files are, depending on whether they concern sensitive data within the meaning of Article 8 of the law, created by decree of the Council of State or by order. But at the *a* priori control stage, the requests for opinions addressed to the CNIL may not include all the information normally required by Article 30 of the law. Similarly, pursuant to point III of Article 26, the acts establishing the creation of these files may, by decree of the Council of State, be exempted from publication in the Official Gazette of the French Republic.

Regarding *a posteriori* control, these files can be exempted, upon specific indication, from the control of the CNIL. It cannot thus lead to general and impersonal control of the overall operation of the data processing (Article 44 of law of 1978). **The processing operations derogating from the general system of the law of 6 January 1978** are currently listed in **decree no. 2007-914 of 15 May 2007,** which shows that the various exemptions are not systematically combined.

Thus, currently, the decree states that:

- 11 files are entitled to a simplified system of advance notification of the CNIL,

- 9 files are characterised by the absence of publication of the regulatory acts creating them;

[120] See provisions of Articles 26, 41 and 44 of law no. 78-17.

- 8 of these files are beyond the general power of *a posteriori* control of the CNIL.

In addition, the exercise of rights by the persons affected by these files is also subject to a derogation system. Article 32-V thus provides for the absence of advance notification, to the extent that such limitation is necessary to meet the purposes of the processing operation (for example, as regards intelligence). Similarly, the right of access is governed by a specific procedure laid down in Article 41 of the law of 1978: the right of indirect access, which requires the person concerned to exercise his right of access through a member of the Commission chosen from the high courts (Council of State, Court of Cassation or Court of Auditors). These must, at the request of any person concerned, carry out checks on behalf of the latter with the competent authorities and, where appropriate, make the necessary corrections.

The bodies benefiting from such derogations are:

I- On the one hand, the relevant bodies in matters of intelligence, in particular, the six departments constituting the "French intelligence community":

Falling directly under the Ministry of Defence:

1) The Direction générale de la Sécurité extérieure (DGSE)[121] [General Directorate for External Security], in charge of espionage and counterespionage outside the national territory.

2) The Direction de la protection et de la sécurité de la défense (DPSD)[122] [Directorate for defence protection and security], responsible for the safety of military personnel, sensitive facilities, information, and equipment.

Falling under the Chief of Army Staff, within the Ministry of Defence:

3) The Direction du Renseignement militaire (DRM)[123] [Directorate of Military Intelligence], in charge of tactical and strategic intelligence in current and future areas of army operations.

Falling directly under the Ministry of Interior:

4) The Direction générale de la Sécurité intérieure (DGSI) [General Directorate for Internal Security], in charge of counterespionage and counter-terrorism operations.

Falling under the Ministry of Economy:

5) The Direction nationale du renseignement et des enquêtes douanières (DNRED)[124] [National Directorate of Intelligence and Customs Investigations] with national jurisdiction, responsible for customs investigations and movement of dubious goods (including fight against the major

[121] Articles D. 3126-1 to D 3126-4 of the defence code.

[122] Articles D. 3126-5 to D 3126-9 of the defence code.

[123] Articles D. 3126-10 to D. 3126-14 of the defence code.

[124] **Order of 29 October 2007 establishing a national department called the "national directorate of intelligence and customs investigations".**

customs fraud, organised crime and trafficking of all kinds - drugs, weapons or other goods -, whose circulation is facilitated by globalisation).

6) The Traitement du renseignement et de l'action contre les circuits financiers clandestins (TRACFIN) [Unit for intelligence processing and action against illicit financial networks], with national jurisdiction, responsible for intelligence on dubious and illegal financial networks. Tracfin is a department that is supported by declarations that certain professions are required to make, especially in the banking sector.

Example of intelligence files:

This includes, in particular and for illustrative purposes, the automated processing of personal data concerning state security, defence or public security approved by the following regulatory acts[125]:

- Decree establishing automated processing of personal data referred to as CRISTINA for the benefit of the General directorate of internal security;

- Decree on the application of Article 31 of law no. 78-17 of 6 January 1978 to the personal information files used by the General directorate of external security;

- Decree authorising the implementation by the Directorate for defence protection and security of automatic processing of personal data referred to as SIREX;

- Decree implementing the provisions of Article 31 of Law No. 78-17 of 6 January 1978 to the personal information file used by the Directorate of military intelligence;

- Order relating to the automated processing of personal information - "the DGSE file" - used by the General directorate of external security;

- Order relating to the establishment of a system for automated processing of personal data referred to as STARTRAC used by the national department TRACFIN...

II- On the other hand, the police and gendarmerie departments as well as judicial authorities are also affected by these derogation:

Examples of processing of personal data used by the judicial police authorities:

The right to criminal investigation files was completely overhauled by Articles 11-15 of law No. 2011-267 of orientation and programming for the performance of internal security (LOPPSI) of 14 March 2011 which introduced, under Title IV of Book I of the Code of Criminal Procedure, two new chapters II and III.

[125] For an exhaustive list, refer to the provisions of **Decree No. 2007-914 of 15 May 2007 adopted for the implementation of I of Article 30 of Law No. 78-17 of 6 January 1978 relating to data protection and privacy.**

Four categories of criminal investigation files - besides the **fichier national automatisé des empreintes génétiques (FNAEG)** [National automated database for genetic fingerprints] whose system remains unchanged - are now governed by the Code of Criminal Procedure:

- The **police record files** governed by Articles 230-6[126] to 230-11; The processing of judicial police records - PJPR - governed by R. 40-23 to R. 40-34 of the Code of Criminal Procedure: replacing the STIC and JUDEX files from which it derived all the data; it is common to the police and gendarmerie units. Two judicial authorities - the public prosecutor and the contact judge - are now responsible for monitoring the PJPR, the CNIL naturally retaining the one assigned to it by the law of 6 January 1978.

- The **serial analysis files,** governed by Articles 230-12 to R. 230-18 and R. 40-35 to 40-37 and the framework decree no. 2013-1054 of 22 November 2013 concerning the automated processing of personal data referred to as "judicial police serial analysis bases", and for establishing connections between data derived from different judicial proceedings, such as the Violent Crime Linkage Analysis System (ViCLAS).

- The **missing persons file,** governed by Article 230-19 and by decree no. 2010-569 of 28 May 2010 (uncodified).

- The **legal harmonisation software**, governed by Articles 230-20 to R. 230-27 and R. 40-39 to 40-41, and to facilitate, within a given procedure, duplication of information.

<u>Examples of processing of personal data used by the judicial authorities</u>:

- "CASSIOPEE" processing: implemented in the district courts, it allows the recording of information relating to complaints and information received by magistrates in the context of judicial proceedings, to improve the processing time of procedures, and ensuring provision of information to victims. The Ministry of Justice is responsible for this processing, which is under the control of a public prosecutor. The right of access and rectification is exercised with the public prosecutor.

- Decree no. 2014-1162 of 9 October 2014 establishing automated processing of personal data referred to as "Plate-forme nationale des interceptions judiciaires" (National interception platform):this is a centralised tool whose purpose is to record and

[126] Under the terms of Article 230-6 of the Code of Criminal Procedure. "In order to facilitate the finding of violations of criminal law, the collection of evidence of these violations and the search for perpetrators, the national police and gendarmerie services can implement automated processing of personal data collected: /1. During the preliminary investigation or expedited police investigations carried out upon letter rogatory and pertaining to any crime or offense as well as fifth-class offences sanctioning: /a) Disruption of public security or tranquillity; /B) Harm to persons, property or authority of the State; /2. During the search for causes of death mentioned in Article 74 or the causes of loss listed in Article 74-1. / These processing operations are also intended for the use of the information collected for purposed of statistical research".

provide magistrates, judicial police officers and agents of the gendarmerie and the national police as well as customs officers and tax departments authorised to conduct judicial investigations, with the content of the intercepted electronic communications and the data and information provided by electronic communications operators and the technical service providers in response to requisitions. This decree comes within the scope of Article 41 of the law of 6 January 1978 (indirect right of access).

8. Subjectively identify the most emerging current problems that arise from processing of personal data by aforementioned security, law enforcement and/or defence institutions. Where appropriate, illustrate by examples.

Response:

Recent events illustrate the difficulty of **balancing the right to privacy and the protection of personal data with the right to security and the protection of public order**.

France has been recently condemned by the European Court of Human Rights (ECtHR), in a chamber judgment of 18 September, "Brunet v. France" (request no. 21010/10), for **its handling of a highly important police file, the STIC** ("système de traitement des infractions constatées") [System for processing reported offences], which has since been replaced by the TAJ ("Traitement d'Antécédents Judiciaires") [Processing of judicial police records]. The process concerns the registration of a French national in this file, after no further criminal proceedings against him. The ECtHR considers, in particular, that it was not actually possible for the person concerned to ask for the deletion of information concerning him from the file and that the shelf life of these data, fixed at twenty years, is a standard duration rather than the maximum duration. In addition, it noted that in 2009 (at the time of the facts), no appeal seemed to be exercised against the decision by the public prosecutor not to proceed with the deletion, since it was only in 2013 that the administrative court acquired the jurisdiction to consider a request to this effect (CS 17 July 2013, "Mr. Elkaim", No. 359417).[127] The Court concluded that "*the respondent State has exceeded its discretion in the matter, since the system for preservation of records in the STIC, as was applied in the case of the applicant, failed to strike a fair balance between the competing public and private interests.*"

The current arrangements for managing the TAJ file, successor to the STIC, created by decree no. 2012-652 of 4 May 2012, helps correct minor errors encountered with the STIC, stipulating in particular that all the decisions to discontinue the case without follow-up will now be mentioned. In the absence of any regulatory provision for appeal against the decision of the magistrate in charge of the file refusing the deletion of information requested by an individual involved, the Council of State has reiterated its jurisdiction to hear such an action: refer to recent decision of the CS 11 April 2014, "Ligue des droits de l'homme", No. 360759. This decision also held that "the collection, preservation and consultation of photographs" taken from this file are compatible with the provisions of Article 8 of the European Convention on Human Rights guaranteeing the right to privacy.

[127] See the decision of the **CS, 17 July 2013, M. Elkaim », no. 359417**.

Finally, it considered that "the retention periods set by the contested decree"[128] which "are based on the severity and criminal category of the respondents", "do not exceed, (...) which is necessary to effectively meet the purposes of the processing", "subject to (...) the accuracy of processed data and their regular updating".

Furthermore, as regards **the monitoring of electronic communications by public authorities,** the principles have been laid down by law no. 91-646 of 10 July 1991 concerning the secrecy of correspondence transmitted through electronic communications. It reiterated the secrecy of communications and has allowed it to be undermined in only two cases: by decision of the judicial authority or, "in exceptional cases" and for purposes defined by law, by decision of the Prime Minister and under the Commission nationale de contrôle des interceptions de sécurité (CNCIS) [National commission for the control of security intercepts]. However, since that date, the practices of communications surveillance by public authorities and their context has changed dramatically, sparking considerable debate about their relevance. They are currently driven by exogenous factors in France: **the order "Digital Rights Ireland" of 8 April 2014 of the CJEU** (Case C-293/12) challenged the European framework for data retention; the revelations of what is referred to as the "Prism case" have, all over the world, brought these issues to the forefront of public debate.

While the judicial interceptions are fully in line with the missions of the judicial police, the administrative interceptions are part of an approach to prevent organised crime, terrorism and other threats against national security. Unlike traditional police tasks, which are to find the perpetrators of offences already committed or to fight against proven threats to public order, the action of intelligence services may relate to information that may or may not be useful that the time of its collection and that will be retained for future duplication.

In the presence of threats that are diverse and difficult to predict faced by countries like France, the functions of analysis and acquisition of information both constitute one of the major priorities of the French national security strategy. These choices have been enshrined in **the military programme law of 29 July 2009 and 18 December 2013**[129], passed under two different political majorities. In the context of a stable overall defence budget and decreasing manpower of the armed forces, the human and financial resources available to the intelligence services is rising sharply.

[128] Article R. 40-27 of the Code of Criminal Procedure resulting from the contested decree sets out, for the adult defendants, an ordinary retention period of twenty years and derogatory periods of five and forty years.

[129] More and more criticism emerging from civil society, particularly from associations seeking to protect the privacy of citizens, and therefore, their personal data which may be the subject of special processing operations, given the development of digital technologies. Thus, the association "La Quadrature du Net" has brought before the Council of State an appeal against the decree implementing the 2013 programming law, which relates to administrative access to login data (decree no. 2014-1576 of 24 December 2014 concerning the administrative access to login data).

"Electromagnetic intelligence", military terminology to denote the interception of electronic communications, is qualified by the report attached to the law of 18 December 2013 as an "essential component of the overall mechanism".

However, the European legal framework for the retention of electronic communications data has recently been challenged. The Court of Justice of the European Union (CJEU) has, by its decision "Digital Rights Ireland" mentioned above, declared Directive No. 2006/24/EC of 15 March 2006 to be invalid, providing for a general obligation of retention of login data of their users for communications operators for a period of six months to two years. It has, in particular, ruled on the metadata sensitivity and the extent of the interference with the rights to privacy and protection of personal data that their systematic conservation represents. This judgment thus raises the question of the possibility to continue applying national laws to data retention and that of the framework which must be defined to replace Directive no. 2006/24/EC. In order to draw - at least initially - consequences from the "Digital rights" judgment, the annual study of the Council of State on *Digital technology and fundamental rights* - already cited under the response to Question 5 - has advocated an immediate review of French laws (including law no. 91-646 of 10 July 1991 concerning the secrecy of correspondence transmitted by means of electronic communication) to strengthen safeguards for fundamental rights without undermining national security.

The French public authorities also intend to **amend the legislative framework for the fight against terrorism**[130]: a draft intelligence law has been presented on 19 March 2015 to the Council of Ministers. It includes in particular the provisions amending the law of 10 July 1991 mentioned above, to include technological changes like mobile phones or the Internet. It defines the mission of the specialised intelligence services and the conditions under which these services may be authorised, for the collection of intelligence relating to exhaustively listed public interests, to use techniques pertaining to administrative access to login data, security interceptions, tracking, sound management of certain places and vehicles, capturing of images and computer data as well as international surveillance measures. It establishes for all of these techniques, except for international surveillance measures, a prior authorisation system of the Prime Minister after notice and under the control of an independent administrative authority referred to as the "National commission for control of intelligence techniques", succeeding the CNCIS, which can receive complaints from any person having a direct and personal interest in the matter. It sets the retention periods for the data collected. It establishes recourse to judicial settlements before the Council of State open to any person who has a direct and personal interest in the matter, and the CNCIS, while providing for derogatory procedural rules designed to preserve the confidentiality of national defence.

The Council of State, which was referred this draft law on 20 February 2015 and 5 March 2015**, gave** - *in its most solemn advisory bench, the general assembly* **- an opinion on 12 March**. In its review, the Council particularly ensured that the necessities

[130] It will in particular be intended to introduce in the legislative part of the code of internal security, a **Book VIII titled:** "**Intelligence**".

specific to the objectives pursued are reconciled, in particular that of the protection of national security, and respect for the privacy protected by Article 2 of the Declaration of human and citizen rights and Article 8 of the European convention on protection of human rights and fundamental freedoms.

In particular, according to the Council of State, the exhaustive and precise definition of the objectives allowing the use of intelligence techniques under the draft law, some of which entail a strong invasion of privacy, is the main guarantee that these techniques will be implemented only for **legitimate reasons.** It thus estimated that these objectives were to be set out **in specific terms** to ensure the effectiveness of the various controls under the draft law by removing formulations whose contours were uncertain. The Council of State, noting the option of the Government to define a single list of objectives applicable in the country and abroad, has selected the following list:

- National security;

- Essential interests of foreign policy and the enforcement of France's European and international commitments;

- Key economic and scientific interests of France;

- Prevention of terrorism;

- Prevention of reconstitution or maintenance of a group dissolved under Article L. 212-1 of the code of internal security[131];

- Prevention of crime and organised crime;

- Prevention of collective violence likely to seriously undermine public peace.

The draft law introduced on 19 March 2015 to the Council of Ministers has included the entire list.

[131] **Article L. 212-1 3 of the Code of Internal Security.** "all the following de facto groups or associations or are dissolved by decree of the Council of Ministers: /1 Those that provoke armed demonstrations on the streets; /2 Or those that are, by their form and military organisation, combat groups or private militias;/3 Or those that aim to undermine the integrity of national territory or undermine by force the republican structure of the government; /4 Or those whose activity tends to thwart the measures for the restoration of republican legality; /5 Or those whose purpose is to either bring together individuals who have been convicted on the authority of collaboration with the enemy, or to glorify this collaboration; /6 Or those that either alleged to have incited discrimination, hatred or violence against a person or group of persons, based on their origin or on their membership or non-membership of an ethnic group, nation, race or religion, or are alleged to have disseminated ideas or theories tending to justify or encourage such discrimination, hatred or violence; /7 Or those that engage, on French territory or from this territory, in activities that cause acts of terrorism in France or abroad. /The maintenance or reconstitution of an association or group dissolved under this article, or the organisation of this maintenance or reconstitution as well as the organisation of a combat group are repressed under the conditions of Section 4 of Chapter I of Title III of Book IV of the Criminal Code".

Furthermore, with regard to the **duration of retention of data collected**, the Council of State desired that it be proportionate to their nature. While, in accordance with its opinion of 3 July 2014 on the draft law strengthening the provisions relating to the fight against terrorism, it has estimated that the retention period for recorded correspondence can be changed from 10 to 30 days, it was also considered necessary that this period begin right now **from the collection of correspondence** and not from the first instance of its use.

The draft law presented to the Council of Ministers also took into consideration this recommendation of the Council of State. This law is currently under consideration by the Parliament.