Balancing the interests in the context of data retention (INVODAS)

France

Elisabeth Quillatre (Legal Adviser – Personal Data Protection, Société Générale and Lecturer – Internet Law, University of Paris 1 Panthéon-Sorbonne)

Part 2: Overarching issues and country-specific questions

A. General part (questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate anonymously?

There is no *"right to communicate anonymously"* as such.

However, *anonymity* is a right, not only by the application of general rules such as the French Civil Code and the protection of Privacy, but also by the application of specific rules such as the French Data Protection Act 1978 or laws related to Internet.

For instance, regarding anonymity related to communication, section 29 of the Act n°2001-1062 of 15th November 2001 on Daily Security (modifying Section L32-3 of the French Posts and Telecommunication Code) states that:

« […] les opérateurs de télécommunications […] sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée […] » [Translated literally: Telecom operators have to erase or make anonymous any data related to a communication as soon as the latter is finished].

2. **Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?**

Regarding my answer to question 63 of the first questionnaire: France recently adopted the decree concerning the data retention obligation of host services operators (Decree n°2011-219 of 25 February 2011 relating to retention and communication of data allowing the identification of creators of online content).

However, ASIC (*Association française des services internet communautaires* [literally translated: The French Association of community Internet services] filed an appeal for annulment before the State Council on April 6, 2011. The Association, which includes companies such as Facebook, Google, or Priceminister, considers that the Decree goes beyond the law on the nature of the data involved and that the wording induces data retention much longer than one year because the Decree provides that the countdown is reset when the user modifies or deletes information. The State Council's opinion is expected by the end of the year. To be continued.

To my knowledge, no other improvement / amendment are currently discussed in public.

Quick-freeze option

Once the evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive was published last April, few papers were published in France about the "quick-freeze option".

In its report, the Commission finds that *"most Member States disagree that any of the variations of data preservation could adequately replace data retention, arguing that whilst data retention results in the availability of historical data, data preservation does not guarantee the ability to establish evidence trails prior to the preservation order, does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime"*.

What was said about this paragraph in French papers is that, in a country like France - a state under the rule of law, only suspects should be subject to surveillance measures; whereas as it is nowadays, every person who communicates are monitored.

Moreover, in November 2001, when France adopted the LSQ Act (Law on Daily Security), a French senator (from the socialist party) said that "there are some

unpleasant measures to be taken in emergencies, but I hope we could return to republican legality before the end of 2003".

This is why some associations, politician, etc., see in the "quick-freeze option" a potential alternative to data retention that respect citizens' liberties.

However, to my knowledge, this alternative is not yet discussed in public (just few papers on Internet about it, without real debate).

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

The French Criminal Code (*Code penal)* provides, in a section entitled "Obstructing the intervention of justice", offences for which everyone should spontaneously cooperate with public authorities in the detection, investigation and prosecution of criminal offences, including:

- The offense of omitting to report a crime of which it is still possible to prevent or limit *("Any person who, having knowledge of a felony the consequences of which it is still possible to prevent or limit, or the perpetrators of which are liable to commit new felonies that could be prevented, omits to inform the administrative or judicial authorities, is punished by three years' imprisonment and a fine of €45,000").* Section 434-1 of the Criminal Code.

- The offence of obstructing the discovery of the truth by (i) "*modifying the scene of a felony or a misdemeanour either by the alteration, falsification or obliteration of clues or evidence, or by bringing, removing or suppressing any given article"* or (ii) "*destroying, purloining, concealing or altering a private or public document or an article liable to facilitate the discovery of a felony or a misdemeanour, the search for evidence or the conviction of the guilty party"* (punished by three years' imprisonment and a fine of €45,000). Section 434-4 of the Criminal Code.

- The offence of not presenting the evidence that a person is innocent: *"Any person who, having evidence that a person provisionally detained or sentenced for a felony or misdemeanour is innocent, wilfully abstains from presenting the evidence before the administrative or judicial authorities is punished by three years' imprisonment and a fine of €45,000".* Section 434-11 of the Criminal Code.

Sections 434-1 and following of the French Criminal Code are available at the following URL address:

http://legifrance.gouv.fr/affichCode.do;?idSectionTA=LEGISCTA000006165378&cidTexte=LEGITEXT000006070719&dateTexte=vig

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

   The principle governing the rights of persons to refuse to testify / to deliver evidence against themselves in France is the principle of the presumption of innocence, including the right to avoid self-incrimination, and the right to remain silent.

   The right to avoid self-incrimination lies in the European Court of Human Rights case-law in the visa of the Convention, section 6. e.g. : Case Funke v. France, 25 February 1993.

   Furthermore, Article 14g of the International Covenant on Civil and Political Rights states that *"in the determination of any criminal charge against him, everyone shall be entitled […] not to be compelled to testify against himself or to confess guilt"*.

   This Covenant came into force in France on February 4th, 1981 and is directly applicable under article 55 of the French Constitution.

   Moreover, are exempted from the provisions of the sections of the Criminal Code above mentioned (related to the cooperation with public authorities in the detection, investigation and prosecution of criminal offences) the perpetrator or accomplice to the offence that led to the prosecution, as well as the persons bound by an obligation of secrecy under the conditions specified by article 226-13. See sections 434-1 and following of the French Criminal Code.

   Finally, the French Code of Criminal Procedure (section 116) makes it compulsory that when an investigating judge hears a suspect, he must warn him that he has the right to remain silent, to make a statement, or to answer questions.

   These rules include, a priori, data that is to be retained and transmitted under the national law transposing the Directive.

   These rights to refuse to testify / to deliver evidence against themselves do not conflict with data retention because providers obligated to retain data are not exempted from the provisions of the Criminal Code related to the cooperation with public authorities in the detection, investigation and prosecution of criminal offences.

5. **Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?**

Regarding HADOPI, measures to store and to safeguard data protection and data security are provided by the Decree n°2010-236 on 5 March 2010 on the automated processing of personal data authorized by section L331-29 of the Intellectual Property Code (*Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet »).*

Section L331-29 states that the High Authority (Committee for the protection of rights) is authorized to create an automated processing of personal data related to persons subject to proceedings.

Decree n°2010-236:

- Section 3 provides the different periods of retention of the data retained in this processing, according to the actions taken by the High Authority against the person concerned (2 months in case the High Authority decides not to send any warning to the person concerned; 14 months in case the High Authority decides to send the warning letter provided by section L331-25 of the Intellectual Property Code; 21 months in case the High Authority decides to send the warning letter delivered against signature provided by article L331-25 of the Intellectual Property Code; 1 year in case the deliberation recording the infringement is transmitted to the public prosecutor… and so on (section 3).

- Section 4 provides the recipients of the data retained in the automated processing: sworn officials authorized by the President of the High Authority pursuant to section L331-21 of the Intellectual Property Code and members of the Committee for the protection of rights have a direct access to the processing; providers have access to technical data and data relating to measures taken against the person concerned (warning letter and/or decision to suspend Internet access); professional defence organizations and societies for the collection and distribution of rights have access to information relating to the prosecutor referral; judicial authorities are the recipients of the minutes of finding of facts that may constitute an offence.

- Section 5 states that the consultations of the processing are recorded, including the identifier of the consultant, the date, the time and the purpose of the consultation. This information is stored for a period of one year.

- Section 8 states that this automated processing is subject to an interconnection with the automated processing of personal data carried out by professional defence organizations and societies for the collection and distribution of rights, as well as with the processing carried out by providers. It is also stated that the interconnections are performed in a manner ensuring the security, integrity and the monitoring of the data stored.

The Decree is available at the following URL address: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021923996

The data stored as a result of a request for access by habilitated police services as part of investigation on terrorism are stored at Levallois-Perret in Paris Region in a centralized information system of the UCLAT.

Otherwise, as a data controller, HADOPI (and other entitles bodies such as UCLAT) has to respect article 34 of the French Data Protection Act which states that: *"The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties"*, provided that failure to comply with the data security requirement or communication of information to unauthorized persons is publishable by a 5 year imprisonment sentence and a 300.000 Euros fine under section 226-17 of the French Criminal Code.

As mentioned in my answer to the question 40 of the first questionnaire, technical and organisational measures to safeguard data protection and data security are not strictly normalized from a legal standpoint.

However, the French data protection Authority (CNIL) has recently (7 October 2010) released a guide on personal data security, intended to help data controllers to comply with their obligations regarding personal data security and is inspired by international norms of data security.

See answer to question 14 below for more information about the CNIL guidelines on personal data security.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

In 2008, there were 503.437 requests for retained traffic data, and in 2009, there were 514.813 requests.

Source: Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive, available at the following URL address: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

However, to my knowledge, there is no more detailed official information on the transmission of retained data to the entitled bodies.

B. Country-specific questions

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

I think the "quick-freeze option" would be a better alternative to the actual data retention regime. Indeed, as only suspects would be subject to surveillance measures this option would respect citizens' liberties, and in particular the presumption of innocence.

8. Are the data to be retained in accordance with the Directive covered by the secrecy of correspondence, as provided for by the national (constitutional) law of your country?

Yes, data to be retained in accordance with the Directive are covered by the secrecy of correspondence. Indeed, the Decree transposing the Directive excludes from the list of data to be retained the data related to the content of the correspondence exchanged, or information accessed during the communication (section L34-1 V of the French *Code des Postes et des communications électroniques*).

Indeed, the interception of the content of communication, for phone conversations and for emails, remains supervised by the Act n°91-646 on 10 July 1991 on the secrecy of correspondence sent by way of electronic communication.

Moreover, section 223-15 of the Criminal Code penalize acts committed in bad faith consisting in opening, deleting, delaying or deviating correspondence with a one-year imprisonment sentence and 45.000 euros fine.

Finally, section L.32-3 of the French Posts and Electronic Communications Code states that operators, and their staff members, are required to respect the secrecy of correspondence.

9. Is the constitutionally fixed limit to a conferral of national sovereignties to the EU (see your answer to question in any way binding for representatives of your country in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?

I am sorry but I do not understand this question. It may be missing a verb.

10. What considerations during the legislative procedure have led to the deviations between the Directive and the national law in terms of the data categories to be retained (see your answer to question 9 of the first questionnaire: no obligation under national law to retain location data, fuzzier definitions of the data categories etc)? Have the additional obligations for internet service providers and hosting providers to retain certain data under Decree n° 2011-219 been seen as a potential violation of the Directive (as they might undermine the efforts to harmonise data retention in electronic communications on a broad

level), or is the said Decree considered as regulating a completely different matter?

As mentioned in my answer to question 9 of the first questionnaire, the Decree goes less in details when compared to the Directive of 15 March 2006 with regards to the categories of data to be retained, both for telephony and Internet. Nevertheless, that does not mean that there are deviations between the Directive and the national law. In case of doubts regarding the categories of data to be retained, French ISP could always refer to the Directive.

Moreover, the additional obligations for Internet service providers and hosting providers to retain data allowing the identification of on-line content creators under the Decree n°2011-219 have not been seen as a violation of the Directive, but rather considered as regulating a different matter. Indeed, France adopted measures to ensure that data is retained and available for the detection, investigation, and prosecution of criminal offences, for the sole purpose of providing judicial authorities with information needed, and also for the prevention of acts of terrorism and protecting intellectual property, whereas the Directive obliges Member States to adopt measures to ensure that data is retained and available only for the purpose of investigating, detecting and prosecuting serious crime.

11. **Could you explain under which law retained data may be used in civil actions (see your answer to question 15 of the first questionnaire) and what steps a litigant and/or defendant must follow in order to be able to introduce these data into the trial? May the litigant and/or the defendant have access to the actual data, or is it only the court that would obtain the data from the provider?**

The French law on evidence has been amended by the Act n°2000-230 of March 13th, 2000. This Act introduced new articles in the French Civil Code including:

- Section 1316 defining a documentary evidence, or evidence in writing, as *"resulting from a sequence of letters, characters, figures or of any other signs or symbols having an intelligible meaning, whatever their medium and the ways and means of their transmission may be";*
- - Section 1316-1 stating that *"a writing in electronic form is admissible as evidence in the same manner as a paper-based writing, provided that the person from whom it proceeds can be duly identified and that it be established and stored in conditions calculated to secure its integrity"*.
- - Section 1316-3 stating that *"an electronic-based writing has the same probative value as a paper-based writing"*.

These new provisions are available at the following URL address: http://195.83.177.9/code/liste.phtml?lang=uk&c=22&r=478#art4380

Thus, retained data are admissible as evidence, provided that the person from whom it proceeds can be duly identified and that it can be established and stored in conditions calculated to secure its integrity.

Concerning the introduction of retained data into a trial in case of civil actions, the litigant will first have to justify of legitimate grounds and request a judicial order, as a preliminary measure, to obtain access to retained data (generally based on IP address collected as an evidence, in order to identify an individual infringing an intellectual property right or personality rights).

The new provisions of the Civil Code above mentioned have few consequences for a litigant wishing to obtain access to retained data (by introducing IP address as a proof) and to introduce them into a trial: first of all, he/she will have to introduce the evidence (such as IP address) in a form sufficiently recognizable by the judge (for instance logs). He/she will have to prepare, organize and retain the proof that the evidence authenticates the person that produced it and its integrity. He/she will therefore have to organise a back up of the server that kept the evidence (for instance a backup of the firewall type server that kept the logs) that should be operated by a bailiff or a computer expert eventually approved by a Court.

The judge will then analyse the legitimate grounds and evidence (IP address) introduced by the litigant and decide whether it is appropriate to request the data retained from the provider. Indeed, only the court (through a court order for instance) may obtain the data from the provider.

12. **Are there any rules preventing the same data from being retained more than once (e.g. when the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? If so: please describe the content of these rules.**

    Not to my knowledge

13. **Are you aware of any plans to impose the costs relating to data retention on the convict of a criminal proceeding in which the retained data is used as an evidence? If so: please provide details on the content of such (draft) provisions, the current state of the discussion and when such provisions might be adopted/come into effect in France.**

    Not to my knowledge

14. **Please summarise the content of the CNIL guidelines on personal data security (as mentioned in your answer to question 40 of the first questionnaire) in brief paragraphs on the different memos. What relevance do the guidelines have in practice? Is their application supervised or monitored in any way (e.g. by the CNIL)? Do the guidelines include rules that apply specifically and exclusively to the storage and transmission of data in the context of data retention? If so, please provide details on these rules.**

    These CNIL guidelines on personal data security are available at the following URL address:
    http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf (in French)

As mentioned in my answer to question 40 of the first questionnaire, this CNIL guide contains 17 memos including the following themes: security risks, user authentication, Management of access, Backup, Maintenance, premises safety, network security, archives, the exchange of information with other agencies, IT development, encryption etc.

Each memo is divided into three sections: (i) basic precautions, (ii) what not to do, (iii) to go further.

Among all recommendations, some are good practices on management of information systems security, while others result from the rules on personal data protection (see the details below).

Memo 1: What are the risks?

(i) Basic precautions:
- To make an inventory of personal data files and associated processing, automated or otherwise, and to identify the media on which these processing are done;
- To determine how the privacy of individuals could be affected through these media;
- For each processing, to identify and classify impacts on privacy according to the severity in case of violation of confidentiality, availability and integrity;
- To investigate threats on each support and to prioritize them according to their probability of occurrence;
- To consider the risks;
- To implement measures security.

(ii) What not to do:
- To conduct alone a risk analysis;
- To realize an analysis too detailed;
- To choose inappropriate measures.

(iii) To go further:
- To budget;
- To use a method;
- It can also be useful to train the persons in charge of carrying out the risks analysis, as well as to perform a security audit of the IT systems.

Memo 2: User authentication

(i) Basic precautions:
- User logins must be different from those set by default by the software publisher;
- In case of a user authentication based on passwords, their implementation must comply with the following rules: should contain at least 8 characters, should use different types of characters (uppercase, lowercase, numbers, special characters), should be changed regularly (every three months for instance);

- When a password is renewed consecutively to an omission, once the password has been reset, the user should be forced to change it at first connexion in order to personalize it.

(ii) What not to do:
- To communicate its password to others;
- To store its password in a file in plain text or in a premise easily accessible to others;
- To use a password related to a person (eg. name, date of birth…);
- To use the same password for different access;
- To configure software so they can save passwords.

(iii) To go further:
- Regarding authentication mechanisms, please refer to the rules and recommendations available at the following URL address: http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_Authentification_v1_0.pdf
- Regarding the use of cryptography for authentication, please refer to the rules and recommendations available at the following URL address: http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf
- Regarding the use of biometrics for authentication, please refer to the CNIL communication available at the following URL address: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNIbiometrie/Communication-biometrie.pdf

Memo 3: Management of access & User awareness

(i) Basic precautions:
- To define authorization profiles in the system by separating the tasks and areas of responsibility in order to limit access to personal data only to duly authorized users;
- To delete the users' access once they are no longer authorized to access a premise or a resource, as well as at the end of their period of employment;
- To document procedures for operations, to maintain them and make them available to all users;
- To draft an IT Charter and attach it to the internal rules of procedures.

(ii) What not to do:
- To define administrator accounts shared by several people.

(iii) To go further:
- To establish, document and review a policy of access control in connection with the purpose of the processing;
- To classify information so as to separate the sensitive data from others and to adapt the level of security to be applied;
- To send regularly to every users updates of the policies and procedures relevant to their duties;

- To organize training and awareness sessions on IT security;
- To sign a non-disclosure agreement.

Memo 4: Safety of workstations

(i) Basic precautions:
- To limit the number of attempts to access an account;
- To install firewall software, and to limit the communication ports strictly necessary for the proper functioning of the applications installed on the workstation;
- To use an antivirus regularly updated;
- To set up a procedure of automatic locking of session in case the workstation is unused for a given time;
- To display, when connecting to an account, the dates and times of the last connection.

(ii) What not to do:
- To use obsolete operating systems.

(iii) To go further:
- To limit the applications requiring administrator level rights for their execution;
- To limit the services of the operating systems running on the workstation to those that are strictly necessary;
- To install the critical updates of operating systems without delay by scheduling a weekly automatic check;
- To update applications where critical vulnerability have been identified and corrected;
- Regarding viruses, please refer to the document of CERTA available at the following URL address: http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007/

Memo 5: How to secure mobile computing?

(i) Basic precautions:
- To provide means of encryption for the storage of mobile computing devices.

(ii) What not to do:
- To store personal information in mobile devices when traveling abroad.

(iii) To go further:

- When mobile devices are used to collect data roaming (eg PDAs, laptops, etc.), the data stored must be secured and a device lock after a few minutes of inactivity should be set up.

Memo 6: Backups and business continuity

(i) Basic precautions:
  - Regarding backups of data:

- To realize frequent backups to prevent the loss of information;
- To store the backup media on an external site, in fireproof and waterproof safes;
- To combine one or more of the following solutions to secure the backups, either:
  - by encrypting the backups themselves;
  - by encrypting the data at the source;
  - by storing them in a secure location.
- To comply with the security policy for the backups conveying.
    - Regarding business continuity:
- To install a smoke detector and fire extinguishers;
- Hardware should not be on the floor (risk of flood);
- About IT materials:
  - The use of an inverter is recommended for equipment used for critical processing;
  - To set up a storage units redundancy by technology RAID.

(ii) What not to do:
- To keep backups in the same premise than the machines hosting data.

(iii) To go further:
- Regarding business continuity, to proportionate all the global services, such as electricity or water supply related to supported systems, and to check them regularly to prevent any risk of malfunction or breakdown.

Memo 7: Maintenance

(i) Basic precautions:
- To ensure that data will not be compromised during a maintenance operation, by applying one or more of the measures listed below:
  - To record maintenance intervention in a handrail;
  - To supervise maintenance realized by a third party;
  - To configure critical systems to prevent maintenance by remote access.
- To inspect all equipments containing storage media before its disposal to ensure that any sensitive data has been securely deleted;
- For users assistance:
  - To configure tools for remote assistance in order to obtain the prior consent of the user before accessing his/her workstation;
  - The user should also be able to see if the remote access is in progress and when it ends.

(ii) What not to do:
- To install vulnerable applications for remote access.

(iii) To go further:
- To limit or prohibit physical and logical access to diagnostic ports and remote configuration ports;
- Regarding material disposal, please refer to the recommendations of ANSSI available at the following URL address:

http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf

Memo 8: Traceability and management of incidents

(i) Basic precautions:
- To save the logs of users activities, anomalies and events related to security;
- To inform users about the logs saving;
- To set up procedures detailing the monitoring of the use of processing and to conduct periodically a review of the logs;
- The controller must be informed promptly of the possible security breaches;
- In case of fraudulent access to personal data, the data controller should notify the persons concerned.

(ii) What not to do:
- To use the logs for other purposes than to ensure the proper use of the IT system.

(iii) To go further:
- The clocks of the different IT systems of an organism should be synchronized with a reliable time source and defined in advance;
- The controller must be kept posted about the technical vulnerabilities of the systems and undertake appropriate actions to handle the risks associated.

Memo 9: Safety of premises

(i) Basic precautions:
- To limit the access to rooms or offices open to host materials containing data by means of locked doors, or airlocks for the most critical equipments;
- To install anti-intruder alarms and to check them periodically.

(ii) What not to do:
- To undersize or neglect the maintenance of the air conditioning of rooms hosting the machines.

(iii) To go further:
- To set up controls in secured areas to make sure that only the staff duly authorized may access them (authentication devices, visible identification (badge)…).

Memo 10: Security of internal computer network

(i) Basic precautions:
- To limit the network flows to the bare minimum;
- To secure access to the IT systems by means of mobile devices - such as laptops, by setting up VPN connections based on strong cryptographic algorithms;
- To encrypt communication by using SSL protocol with a key of 128 bits during the implementation of web services.

(ii) What not to do:

- To use telnet protocol for the remote connection to active equipments of the network;
- To install WIFI networks.

(iii) To go further:
- The network partitioning allows to prevent that a compromised workstation does not compromise the entire system. In practice, it is recommended to partition the network into logical sub-networks according to the services expected to be deployed;
- To set up intrusion detection systems (IDS) to analyse the network traffic in real time, in order to detect any suspicious activity evoking a scenario of IT attack;
- To set up an automatic identification of materials as means of authentication of the connections from specific equipments and areas (eg. MAC address).

Memo 11: Security of servers and applications

(i) Basic precautions:
- To change passwords by default by complex passwords that should respect at least the following rules: passwords should have a size of 10 characters minimum, they should use different types of characters (capital letters, numbers, special characters..), they should be changed at the departure of one of the administrators;
- To install critical updates of operating systems without delay by scheduling a weekly automatic check;
- As regards databases administration: the servers hosting databases should not be used for other purposes, personal accounts should be used to access to the databases, measures to protect attacks by integration of SQL code should be set up, specific measures for "sensitive" databases should be put in place;
- To ensure continuity of data availability, which requires particular precautions when installing or updating software on operating systems;
- To update applications where critical breaches have been identified and corrected.

(ii) What not to do:
- To use non-secure services (authentication in plain text, flows in plain text…);
- To host databases in an area directly accessible from Internet.

(iii) To go further:
- Sensitive systems shall have a dedicated environment;
- Regarding software running on servers, vulnerability detection tools shall be set up;
- According to the nature of the application, the integrity of the processing may be ensured by using signatures of executable code ensuring that it has not been altered.

Memo 12: Subcontracting

(i) Basic precautions:
- To include in the contracts between the data controller and its subcontractors a specific clause covering the confidentiality of data;
- To make arrangements (security audits, visit on sites, etc.) to ensure the effectiveness of the guarantees offered by the subcontractor regarding data protection (encryption of data, encryption in transfer, traceability etc.);
- To determine the conditions of data retrieval and destruction in case of termination or end of the contract.

(ii) What not to do:
- To use services providing IT functionalities without warranty regarding the actual location of data.

(iii) To go further:
- For data concerning health, the hosting provider shall have a license issued by the Minister of Health. For more information, please refer to the website of the Minister of Health available at the following URL address: http://esante.gouv.fr/.

Memo 13: Archiving

15. Basic precautions:
- To implement specific procedures for access to archived data;
- To follow recommendations given in the memo 17 regarding the encryption of archives;
- Regarding the destruction of archives, to adopt a procedure ensuring that the entire archive has been destroyed.

16. What not to do:
- To use media that does not offer sufficient guarantee of durability.

17. To go further:
- More information on archival issues are available on the "Archives de France" website available at the following URL address: http://www.archivesdefrance.culture.gouv.fr/gerer/archive-electroniques/

Memo 14: Exchange of information with other organization

(i) Basic precautions:
  - Regarding the confidentiality of communication
- To encrypt data before saving it on a media when the communication of data is performed by sending a physical medium;
- When sending the data via a network: (i) if the transmission uses email, it is recommended to encrypt the files to be transmitted; (ii) in case of a file transfer, it is recommended to use a protocol guaranteeing the confidentiality of data (such as SFTP); (iii) if the transmission uses HTTP, it is recommended to use

SSL protocol (HTTPS) to ensure authentication of the servers and confidentiality of the communication;
- In all cases, the transmission of the secret (decryption key, password, etc.) guaranteeing the confidentiality of the transfer shall be done via a separate transmission, and when possible through a channel of different nature that the one used for the transmission of data.

(ii) What not to do:
- To transmit files containing personal data in plain text via webmail such as Gmail or Hotmail.

(iii) To go further:
- Regarding data integrity, it is recommended to calculate the mark on the data in plain text and to transmit this mark so as the integrity of data can be checked when received.
- Regarding the authenticity of the data, the sender can sign the data before sending them so as to ensure that he/she initiated the transmission.
- Once the data have been received, that their integrity has been checked by the recipient and have been integrated into the IT system, it is recommended to destroy the files or media used for the transmission.

Memo 15: IT developments

(i) Basic precautions:
- To perform software development in an environment distinct from the production one;
- To take into account security requirements towards personal data from the development of the service or from the design of the application.

(ii) What not to do:
- To use real personal data for the development and test.

(iii) To go further:
- The development shall impose format for data input and storage which minimize the data collected;
- Data formats shall be compliant with the implementation of a data retention;
- The access control by category shall be integrated at the development;
- To avoid fields of free texts.

Memo 16: Anonymization

(i) Basic precautions:
- To be very vigilant as far as a re-identification can be done from partial information;
- To anonymize a personal data as follows: to generate a secret sufficiently long and difficult to memorize; to apply a one-way function on data (hacking algorithm with secret key);

- If a data is anonymized instead of deleted, there is a risk of re-identification: to set-up organizational measures to guarantee the confidentiality of the secret.

(ii) What not to do:
- To use mechanisms for anonymization non validated by experts. A good anonymization algorithm must be irreversible, have a very low rate of collision, have a wide dispersal, implement a secret key.

(iii) To go further:
- In some cases, it is recommended to apply a double anonymization.

Memo 17: Encryption

(i) Basic precautions:
  - Regarding the symmetric encryption:
- To use algorithms at the state of the art, such as AES or triple DES;
- To use cryptographic keys at least 128 or 256 bits and not weak.
  - Regarding asymmetric encryption:
- To use proven algorithms such as RSA or ECC;
- Regarding the key length, please refer to the recommendation given in Annex B1 of the *"Référentiel Général de Sécurité"* available at the following URL address: http://www.references.modernisation.gouv.fr/rgs-securite.

(ii) What not to do:
- To use a simple DES algorithm, considered as obsolete;
- To use cryptographic software that have not been audited by expert third parties.

(iii) To go further:
- Encryption of documents can be achieved with different software, including TrueCrypt software, Gnu Privacy Guard software, or by default, 7-ZIP software.

However, there is no rule that apply specifically and exclusively to the storage and transmission of data in the context of data retention.

As mentioned above, these are only guidelines / recommendations (not legally binding).

However, as indicated in this guide, the CNIL supervises compliance with the law, by inspecting IT systems and applications. The CNIL uses its inspection and investigation powers in particular to check that all precautions are taken to prevent the data from being distorted or disclosed to unauthorized parties.

Thus, in a sense, we can say that the application of these guidelines is supervised by the CNIL.

18. As regards the protocols between providers and the Ministry on data storage and transfer under Decree n° 2007-1538 (cf. your answer to question 29 of the first questionnaire): are these protocols agreed upon every time a data request

is made, or on a general basis for all data that is requested from one particular provider? If the latter:

The protocols between providers and the Ministry on data storage and transfer under Decree n°2007-1538 are agreed on a general basis for all data that is requested from one particular provider.

- **which details regarding technical and organisational measures laid down in these protocols are known to you?**

  I do not have access to any details regarding technical and organisational measures laid down in these protocols.

  All I know is that modalities according to which the organism or legal person allow the police officer to access the data retained and to transfer them by electronic means to the relevant police service, as well as the terms and conditions for securing the electronic connexion in order to ensure the origin, the destination, integrity and confidentiality of data during the transmission of the data to the requesting service are detailed in these protocols.

  Moreover, a copy of the protocol is transmitted to the CNIL in connection with the formalities prescribed by the French Data Protection Act n°78-17.

- **Which conclusions on the content of the measures (potentially) regulated by these contracts might be drawn from statements made in the media or the public debate?**

  To my knowledge, no statement on the content of the measures regulated by these protocols has been made in the media or the public debate.

  Indeed, as indicated above, only the CNIL and police officers duly authorized to access to the retained data have access to the content of these protocols and thus to the details regarding technical and organisation measures laid down in these protocols.

- **Do you have any information with how many and which providers *direct* access to the retained data has been agreed upon?**

  The only information I have is that in 2008, there were 503.437 requests for retained traffic data, and in 2009, there were 514.813 requests (see my answer to question 6 above).

19. **As regards your answers to questions 29 and 43 of the first questionnaire: Please add details on the rules and practices governing the co-operation between the party retaining the data and the party (public authority) accessing them in case a data request is made by *HADOPI* or (upon a court order) in a *civil action*.**

As mentioned in my answer to question 15 above, modalities according to which the organism or legal person allow the police officer to access the data retained by the provider and to transfer them by electronic means to the relevant police service are detailed in the protocols between providers and the Ministry on data storage and transfer under Decree n°2007-1538.

Moreover, the Decree n°2010-872 on July 26, 2010 details the procedure before HADOPI Committee for the protection of rights (introducing section R331-35 and following in the French Intellectual Property Code), including the following provisions:

Section R331-35 states that to be eligible, referrals to the HADOPI Committee for the protection of rights shall include personal data and information specified in Annex 1 of the Decree n°2010-236 of 5 March 2010, as well as an affidavit according to which the author of the referral acts on behalf of the rights holder. Upon receipt of the referral, the Committee on Protection of Right acknowledges receipt by electronic means.

Section R331-37 states that the providers are required to disclose personal data and information specified in the annex of he Decree n°2010-236 within eight days following the submission by the Committee of technical data needed to identify the Internet user / subscriber whose access to online communication services was illegally used (failure to do so is punishable by a fine for contraventions of the fifth class).

This decree is available at the following URL address: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022518612&fastPos=1&fastReqId=1586631039&categorieLien=id&oldAction=rechTexte

20. **Please describe the rules for co-operation among the different bodies accessing the data and between these and other public authorities in detail: Are there any provisions that allow the bodies entitled to obtain access to the data retained to transfer these data, once obtained, to other authorities for their respective purposes? If so, please describe the requirements that have to be fulfilled for such transfer, and how data exchange between them is effected in practice?**

There are no specific provisions that allow the bodies entitled to obtain access to the data retained to transfer these data to other authorities for their respective purposes.

However, there are rules governing the cooperation in between authorities of the Member States such as the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of

police and judicial cooperation in criminal matters which sets forth the rules applicable to the transfer of personal data between authorities of the Member-States in charge of investigation and prosecution of crimes.

21. **As far as I understand from your answers to question 14, 16 and 35, in criminal and civil cases, access to the retained data may only be sought subject to a court order, whereas for the purposes of the "Anti-terrorist" Act, a qualified person under the supervision of the Ministry of the Interior and monitored by the CNCIS, may order that the data be requested. In the case of HADOPI, however, there seems to be no independent body (such as a judge or the CNCIS) monitoring compliance of the authority's orders with the law, which would mean that the decisions of HADOPI may only be controlled *ex-post* in a court proceeding. Is this understanding correct? If not, please explain the situation.**

HADOPI (High Authority for the dissemination of works and the protection of rights on Internet) is an independent public authority. To this end, it is granted authority to appear legally as an entity ("moral personality") (Section 331-12 of the French Code of Intellectual Property).

Indeed, HADOPI may request access to data retained by ISP after receipt of a complaint from a copyright holder or a representative in order to identify the Internet user and send him/her a "warning letter" (injunction referring to section L336-3 of the Intellectual Property Code, enjoining him/her to respect the requirement defined by this section and warning him/her of the sanctions if the presumed violation continues).

In case of repetition of acts that may constitute violation of the obligation defined in section L336-3, cases will be transmitted to the justice.

The validity of injunctions pronounced by the High Authority may not be contested except by appeal for recourse directed against a decision to sanction pronounced by a judge in application of section L331-27.

Balancing the interests in the context of data retention (INVODAS)

France

Elisabeth Quillatre (Legal Adviser – Personal Data Protection (Société Générale; Lecturer – Internet Law (University of Paris 1 Panthéon-Sorbonne)

Jean-Baptiste Thomas Sertillanges (Associate at Herbert Smith LLP; Lecturer – Internet Law (University of Paris 1 Panthéon-Sorbonne)

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. **Have the provisions of the Directive already been transposed into national law?**

Yes.

The main provisions consisting in establishing a data retention obligation for providers of publicly available electronic communications services (hereinafter "internet services providers") were already part of the telecommunication regulation framework since the enactment of Act n°2000-1062 of 15th November 2001 on Daily Security, section 29 (hereinafter the LSQ Act).

This obligation was originally part of the Bill for Information Society n°3143 of 14th of June 2001 (sections 14 to 16), but it had to be implemented during the following legislature with the LSQ Act.

Even before, under section 126 of the French Posts and Telecommunication *Code (Code des Postes et des Communications Electroniques*), France Telecom - the national telecommunication operator at that time - was entitled to retain communication data for invoicing purposes for one year, corresponding to the opposability of invoices to consumers.

The LSQ Act provides that Internet services providers can delay the erasure or anonymization of traffic data up to one year for the purpose of criminal prosecution, invoicing and provision to consumers of consented added-value services.

Data retention for criminal prosecution thus became an obligation, applicable to all competing telecommunication operators, as specifically the main objective of the LSQ was to facilitate the prosecution of criminal activity and fight against terrorism.

However, the specific provisions of the Directive, in particular those normalizing the categories of data to be retained were implemented in national law by the Decree n°2006-358 of 24th of March 2006 regarding the retention of electronic communication data. The French version of the Decree can be found under http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000637071&dateTexte=&categorieLien=id.

The Decree has been codified in the French Posts and Telecommunication Code (section R10-12 and seq.).

This application Decree was awaited, insofar as, since the enactment of the LSQ in 2001, nothing existed to determine precisely the categories of data to be retained, the exact period or retention or the compensation of costs incurred by operators. Indeed, the LSQ referred to a decree of application, to be taken after a consultation of the French Data Protection Authority, and addressing these issues but was never taken before 2006.

Apart for the general principle established by the LSQ Act, the Decree n°2006-358 of 24th of March 2006 constitutes the official legal text implementing the Directive in French law.

Other legal texts are linked to data retention:

- Act n°91-646 of 10 July 1991 relating to the secrecy of correspondence sent by way of electronic communication;
- Act n°2004-575 of 21 June 2004 on Trust in Digital Economy (article 6-2 and article 22) – transposing the directive 2000-31-EC on electronic commerce;
- Act n°2004-669 of 9 July 2004 on electronic communications and audiovisual communication services;
- Act n°2006-64 of 23 January 2006 on the fight against terrorism (the Anti-terrorism Act);
- Decree n°2006-358 of 24 March 2006 on the retention of electronic communication data;
- Decree n°2007-1145 of 30 July 2007 on the creation of an automatic processing of personal data referred to as "transmission system of judiciary interception";
- Decree n°2007-1538 of 26 October 2007 on the communication of data by electronic mean and amending the Code of criminal procedure (as amended by the Decree 2008-150 of 19 February 2008);
- Act n°2009-669 of 12 June 2009 on the promotion of the dissemination and the protection of creation on the Internet.
- Decree n°2011-219 of 25 February 2011 on relating to retention and communication of data allowing the identification of creators of online content

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?

/

3. Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?

/

4. In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.

/

- ***If transposition has been <u>accomplished</u>:***

General questions

5. Is there an English version of the texts available? If so: Please indicate the respective URL.

No, there is no English version of the Decree n°2006-358 of 24 March 2006 to our knowledge published on official websites. There may be unofficial translations available but we have not identified them.

6. Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?

In France, legal texts are published in the Official Journal of the French Republic to ensure enforceability. In the absence of special and/or transitory provisions, it comes into force the day following its publication.

The Decree n°2006-358 was published in the Official Journal on 26th March 2006, and thus came into force on 27th March 2006. There was no transition period.

7. What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe

The Directive has been mainly implemented by an application decree taken by the government.

However, the general data retention obligation borne by Internet service providers was established by an Act of parliament (*Loi*) and the decree provisions stand as supplementary rules meant to set forth the practical modalities of application of the law.

a) Whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and

Yes. Under the French Constitution, some enumerated "important matters" are to be enacted by the Parliament. Complex pieces of legislations increasingly lay down the fundamental rules and principles, while referring to application decrees, to be taken at a latter date during the legislature, and providing details and clarifications as to the practical modalities and procedures of application of legal provisions.

b) Whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.

Yes.

European directives can be implemented into French law either by statutes, ordinances or decrees. The choice is generally made depending on the subject matter, i.e. Parliament having a "reserved domain" on some important issues and the implementation of a European directive into French law has to comply with the hierarchy of norms and the distribution of matters between legislation and regulation.

The Constitution determines matters that have to be dealt with by legislation or by regulation. On the one hand, article 34 of the French Constitution provides a list of matters that have to be dealt with by Parliament statutes, such as civic rights and the fundamental guarantees granted to citizens for the exercise of their civil liberties; freedom, diversity and the independence of the media; the obligations imposed for the purposes of national defence upon the person and property of citizens; the determination of serious crimes and other major offences and the penalties they carry; criminal procedure; amnesty; the setting up of new categories of courts and the status of members of the Judiciary, etc. On the other hand, section 37 of the Constitution provides that "*matters other than those coming under the scope of the legislative shall be matters for the executive*".

With regards to the implementation of the Directive, the choice of a statute to establish a general data retention obligation - an issue related to civil liberties and criminal procedure - and a decree to determine the practical modalities of application is typical of our current system.

8. Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?

The LSQ as subsequently amended and the decree have been codified into the French Posts and Telecommunication Code, where the following terms are defined in section L.32:

Electronic communications; Electronic communications network; Public network; Network endpoints; Local loop; Independent network; Internal network; Electronic communication services; Public telephone service; Access; Interconnection; Terminal Equipment; Radio network, facility or equipment; Essential requirements;

Geographic number; Non-geographic number; Service provider; Satellite system; Local roaming; Ultramarine roaming; Traffic data.

These definitions do not substantially deviate from those referred to in Art.2 para.1 and 2 of the Directive.

The notion of traffic data covers data processed in view of the transmission of a communication through an electronic communication network or in view of its invoicing conformingly to the Directive 2002-58.

Moreover, all the terms mentioned in the Directive 95/46/EC are defined in national law (French Data Protection Act 1978-17 of 6 January 1978 as amended), except "data subject's consent".

Dimension 1 (State - citizen)

9. **What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?**

The data to be retained are defined by the Decree of 24 March 2006 implementing the Directive and specifies the "technical" data to be retained:

(i) Categories of data to be retained for purposes of crime research, finding and prosecution are:

- Information allowing the identification of the user;
- Data related to the terminal equipment used for the communication;
- Technical specifications as well as the date, time and duration of each communication;
- Data related to additional services requested or used and their suppliers;
- Data allowing the identification of the recipient(s) of the communication.
- Concerning telephony, service provider can retain, additionally to the above data, information allowing the identification of the origin and localization of the communication. These data can be retained only if they are necessary for billing and payment purposes.

(ii) Categories of data to be retained for billing and payment purposes are:

- Information allowing the identification of the user;

- Data related to the terminal equipment used for the communication;

- Technical specifications as well as the date, time and duration of each communication;

- Data related to additional services requested or used and their suppliers;

Concerning telephony, service provider can retain, additionally to the above data, information allowing the identification of the origin and localization of the communication, data allowing the identification of the recipient(s) of the communication, as well as data allowing the establishment of bills.

(iii) Categories of data to be retained for network and facilities security purposes are:

- Information allowing the identification of the origin of the communication;

- Technical specification as well as the date, time and duration of each communication;

- Technical data allowing identifying the recipient(s) of the communication;

- Information relating to additional services requested or used and their suppliers.

Nevertheless, the Decree goes less in details when compared to the Directive of 15 March 2006 with regards to the categories of data to be retained, both for telephony and Internet (see answer to question 10).

There is no specification on whether data on unsuccessful call attempts have to be retained.

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

Notwithstanding the traffic data retention obligations to be borne by Internet service providers, host services providers are required to retain traffic data under the Act of 21 June 2004 on confidence in the Digital Economy.

The objective is to ensure freedom of expression by allowing authors to remain anonymous while publishing content, whereas allowing *ex post* identification in specific situations (identifying the author of illegal content) with the help of Internet service providers.

The data to be retained is data identifying the author of content on the Internet i.e. log-in data (ID login, IP address, date and time of log-in and log-off) and administrative data (name and address of the subscriber, and payment method).

Awaiting for since 2004, the decree n°2011-219 of 25 February 2011 specifies the application conditions of article 6 II and II bis of the Act of 21 June, 2004 for the confidence in the digital economy, which requires retention of data allowing the identification of on-line content creators.

The Decree specifies the data concerned, the notion of contribution to the creation of content and the retention period.

For each connection of their subscribers, the **Internet Service Providers** should keep the following data:

- The connection identifier;
- The identifier provided by the service provider to the subscriber;
- The identifier of the terminal used for the connection when this data is available;
- The dates and the hours of beginning and end of connection;
- The characteristics of the subscriber's line.

For each operation of content creation, the **hosting companies** should keep the following data:

- The identifier of the connection at the origin of the communication;
- The identifier provided by the information system to the object content of the operation;
- The type of protocols used for the connection to the service and for the transfer of content;
- The nature of the operation;
- The dates and the hours of the operation;
- The identifier used by the author of the operation when this data is available.

During the subscription of a contract by a user or during the creation of an account, the following data is to be kept:

- The connection identifier at the time of the account creation;
- The name and first name or corporate name;
- The associated postal addresses;
- The pseudonyms used;
- The e-mail addresses or associated accounts;

- The telephone numbers;

- The password and updated information allowing its verification or modification in their latest updated version.

When there is a fee for the subscription of the contract or the account, data concerning the payment should be kept:

- The type of payment used;

- The registration number of the means of payment;

- The amount;

- The date and time of the operation.

Data relating to the subscription of a contract or opening of account by a user, free of charge or not, have to be retained if "usually" collected by the ISP or hosting company.

The decree specifies in its article 2 that contribution to the creation of content refers to initial creations, modifications and removal of content.

Article 3 of the Decree specifies that the retention period is one year. The starting point of this period varies according to the type of operation.

Generally, the principle of secret of correspondences (Law n° 91-646 of 10 July 1991) prohibits recording the content of communications or information accessed to during communication, except in specific situations as provided by article 100 et seq. of the Criminal Procedure Code if the penalty applicable to the suspected infringement is superior to a 2-year imprisonment sentence and authorized by the magistrate in charge of the instruction.

Other data retention obligations on content have been implemented for the purposes of search of information affecting national security, safeguarding the essential elements of scientific and economic potential in France, the prevention of terrorism, crime and organized crime. The Decree of 30 July 2007 thus creates an automatic processing of personal data referred to as "*transmission system of judicial interception*". It allows interception of correspondence (content data) sent through electronic communications in accordance with the French Code of Criminal Procedure.
Under this decree, once the interception has been prescribed or required by magistrates, the following data will be transmitted by electronic communication operators and could thus be retained into the *transmission system*:

- Traffic data (service provider's code, phone numbers and e-mail addresses of those called and callers, date, time, duration and identification of activated connections);

- Content of SMS messages sent or received by a telephone line which is intercepted;

- Data related to recipients of interceptions (e-mail address, telephone numbers of their receiving equipment, and unique identification number assigned to requisition interception.

Moreover, each log-in to the system of judicial interception is recorded (user ID, date and time of the log-in).

The retention of customer records is generally subject to contractual provisions, notwithstanding the general obligations for the data controller and processor to be compliant with the French Data Protection Act n°78-17 of 6 January 1978.

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

1. Under the Decree of 24 March 2006, data may be retained only:
(i) For the purpose of researching, finding and prosecuting criminal offences as well as the fight against copyright infringement;
(ii) For the purpose of billing and payment of electronic communications services;
(iii) For purposes of network security;
(iv) For purposes of the fight against terrorism (Act n°2006-64 of 23 January 2006).

2. Data listed by the Decree of 30 July 2007 may be retained only for purposes of search of information affecting national security, safeguarding the essential elements of scientific and economic potential in France, the prevention of terrorism, crime and organized crime.

3. Data listed by the Act of 21 June 2004 on Confidence in the Digital Economy may be retained only for purpose of identifying perpetrators of illegal content on the Internet.

12. Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?

The Decree transposing the Directive excludes from the list of data to be retained the data related to the content of the correspondence exchanged, or information accessed during the communication.

The French Posts and Electronic Communications Code states that data retention should be carried in compliance with the French Data Protection Act. Section 8 of this Act prohibits the collection and the processing of "sensitive data" (personal data

revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life).

The Law n°91-646 of 10 July 1991 relating to the secrecy of correspondence sent by way of electronic communication protects the content of correspondences, as well as section 223-15 of the Criminal Code that penalize acts committed in bad faith consisting in opening, deleting, delaying or deviating correspondence with a one-year imprisonment sentence and 45.000 euros fine.

Section L.32-3 of the French Posts and Electronic Communications Code states that operators, and their staff members, are required to respect the secrecy of correspondence.

Professional secrecy is protected under section 226-13 and 226-14 of Criminal Code, which penalizes the disclosure of secret information by professionals with a one-year imprisonment sentence and a 15.000 euros fine.

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefor.**

Period of data retention determined by the Decree is one year after their collection. This provision is consistent with those of Article 6 of the Directive that provides a period ranging from six months to two years.

Particularity of the Decree: for the security of networks and facilities purposes, service providers can retain information allowing the identification of the origin of the communication, technical specification as well as the date, time and duration of each communication, technical data allowing to identify the recipient(s) of the communication, and information relating to additional services requested or used and their suppliers for a period not exceeding three months.

Concerning telephony, service provider can retain data only during the time strictly necessary for billing and payment purposes, without exceeding one year.

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

Article 34-1 of the Posts and Electronic Communications Code states that judicial authorities as well as the special authority designed to fight illegal downloading on the Internet (HADOPI) are entitled to access the data retained, as appropriate.

Moreover, under the "anti-terrorist" Act of January 23, 2006, officer, individually designated and duly authorized, working for the French police agencies specifically

responsible for the fight against terrorism, can request the disclosure of information after a formal access request procedure (as explained in question 16)

Private litigants may obtain access to retained data, subject to obtaining a judicial order on a case-by-case basis and if they can justify legitimate grounds (for instance as a preliminary measure in fast-track procedures to identify the author of defamation on the Internet before assessing the case on the merits).

Finally, under the French Data Protection Act 1978-17 as amended, data subject is entitled to interrogate the data controller of personal data in order to know whether the personal data relating to him for part of the processing and, if so, to obtain communication of the personal data relating to him as well as any available information on the origin of the data (section 39).

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?**

Under the Decree implementing the Directive, data retained can be used for purposes of crime research, finding and prosecution; billing and payment purposes; as well as network and facilities security purposes.

Under the decree n°2011-219 of 25 February 2011, data retained can be used to identify the creator of online content.
Apart from these purposes, data retained can be used in order to prosecute criminal offences (including cybercrime), in case of civil actions, such as to enforce copyright claims, defamation, and for the prevention of terrorism by way of administrative requests.

The French Data Protection Act 1978-17 grant a right to individuals to access personal data related to them directly from the data controller – thus, from the Internet service provider.

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

As a general observation, there is no legal criteria or specific ground justifying the access to the data, except a general distinction for (i) prevention of terrorist activities (ii) investigation and repression of crimes (iii) copyright infringement (iv) private litigation entailing the application of specific procedure.

The fact that each access has to be authorized by a specific person means that whether the access is justified will depend on an appreciation on a case-by-case basis with regards to the missions of the authorities, the likelihood of infringement,

the already gathered evidence, the risks at stake, and globally the proportionality of the measure when compared to the objective.

In the case of judiciary requests (for the investigation of crimes), the officers in charge of an investigation must obtain an authorisation by the judge in charge of the instruction of the case or the *Juge des Libertés et de la Détention* (liberty and custody judge).

The *Juge des Libertés et de la Détention* (JLD) has been created by the French Act of June 15, 2000. The JLD is a judge with the rank of presiding judge, of senior deputy presiding judge, or of deputy presiding judge. The JLD is appointed by the presiding judge of the district first instance Court.

- This judge has various functions and tasks, including the following:

- He may order or prolong a remand in custody, or reject a request for release;

- He may impose penalty for failure to comply with a judicial review;

- He may authorize the searches, house visits and seizures of exhibits outside the legal hours in case of organized crimes and delinquency;

- He may extend the *garde à vue* (police custody) beyond 48 hours in case of organized crime and drug trafficking.

In case of suspected terrorist activities, access is granted on a case-by-case basis after a formal access request procedure pursuant to article L.34-1-1 of the French Posts and Electronic Communications Code. Under section R10-17, the request must contain the name and title of the person requesting the access, the name of his unit and his address, the nature of the requested data, and where appropriate, the relevant period. Above all, the request must be duly motivated.

Requests are transmitted by a designated officer (cf. question 14) to a "qualified person" placed under the supervision of the Minister of the Interior - in charge of national security. This qualified person is appointed by the National Commission for Control of Security Interceptions on proposal of the Minister of the Interior for a term of three years. These requests and decisions of the qualified person are recorded and kept for a maximum of one year in an automated processing implemented by the Ministry of Interior.

Approved access requests are then transmitted, without motivation, to the incumbent service provider who must communicate the data to the applicant. These communications of data must be carried out under conditions ensuring their security, integrity and monitoring.

Concerning access requested by individuals in case of civil actions: the plaintiff must justify of legitimate grounds and request a judicial order, as a preliminary

measure, to obtain access to data, generally in order to identify an individual infringing an intellectual property right or personality rights.

HADOPI may request access to data retained by ISP after receipt of a complaint from a copyright holder or representative.

17. Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?

For private litigants, it is required to obtain a court order, insofar as it guarantees an *ex ante* appreciation by the judge of the grounds for access on a case-by-case basis.

A specific procedure allows the plaintiff to obtain a temporary non-contradictory court order (section 495 alinea 3 of the Code of Civil Procedure), a procedure generally used in order to identify the opposing party or the author of the damage, or to investigate and obtain, pursuant to article 145 of the Code of Civil Procedure, evidence of facts before judging the case on the merits. This request procedure is also applicable where, depending on the circumstances, the presence or information of the aggrieved party would compromise, for instance, the efficiency of the ordered measure or entail a risk of proof destruction.

In case of judiciary requests, the officers must obtain an authorization from the magistrate in charge of instruction of the case or from the judge of detention and liberties (Sections 60-2, 77-1-2 et 99-4 of the Code of Criminal Procedure).

A court order is not required for administrative request pertaining to prevention of terrorism but a formal authorization from the "qualified person" placed under the supervision of the Ministry of the Interior (Act n°2006-64 of 23rd January 2006, art. 6 as codified Article L34-1-1 of the French Code of Posts and Electronic Communication).

In case of investigations before the HADOPI for copyright infringement, a court order is not necessary to request access to the data, as the HADOPI will be in charge of handling the request before the operators after receipt of a complaint from a copyright holder or representative.

Except in case of the specific procedure allowing the plaintiff to obtain a temporary non-contradictory court order and in case of investigations before the HADOPI, there is an obligation to hear the aggrieved party before a decision to grant access to the data retained is taken.

This obligation applies also to pre-trial criminal investigations and/or to administrative procedures under the « Anti-terrorist Act ».

The right for the aggrieved party to be heard before a decision to grant access to her data is taken results from the "*contradictory proceedings*" principle. The principle of

"*contradictory proceedings*" is a rule of law existing in any proceedings, whether civil, administrative, criminal or disciplinary:

The "*contradictory proceedings*" principle is provided by sections 14 to 17 of the French Code of Civil Procedure, available at the following URL address: http://legifrance.gouv.fr/affichCode.do;jsessionid=6C67D9037899199966A8D40099FFF751.tpdjo04v_1?idSectionTA=LEGISCTA000006149639&cidTexte=LEGITEXT000006070716&dateTexte=20110810

Moreover, the Preliminary Article of the French Code of Criminal Procedure states that:
"Criminal procedure should be fair and adversial and preserve a balance between the rights of the parties" ("*La procédure pénale doit être équitable et contradictoire et préserver l'équilibre des droits des parties*"). The principle of *"contradictory proceedings"* is also mentioned in several articles of the French Code of Criminal Procedure (for instance, art. 135-2, 137-1, 145 to 145-2, 149, 187-1, 410, 625, 706-53-15, 706-71, 712-3, 712-6, 712-7, 730, 823-1…). An English version of the French Code of Criminal Procedure is available at the following URL address: http://195.83.177.9/code/liste.phtml?lang=uk&c=34

18. Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?

There is indeed a general obligation to notify a data subject prior to the access to data retained, provided by Article 32 of the Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties as amended (the data controller shall provide the data subject with the information enumerated in Article 32(I) such as the recipients and third parties to who the data will be communicated, prior to the recording of data or prior to the disclosure of data to a third party).

The French Data Protection Act is available at the following address (in English): http://www.cnil.fr/english/official-texts/

Regarding access requested by individuals in case of **civil actions**, the plaintiff must justify of legitimate grounds and request a judicial order, as a preliminary measure, to obtain access to the data. This court order guarantees an *ex ante* appreciation by the judge of the grounds for access on a case-by-case basis.

(i) In case of a *non-contradictory* court order under section 495 alinea 3 of the French Code of Civil Procedure, the *Court de Cassation* (final court of appeal) has considered that once ordered, the decision of the measure to be taken (communication of traffic data so as to identity the author of content on the Internet) shall be notified to the aggrieved party before the access to data even if it is seconds before the access (Cass. Civ. 9th April 2009).

(ii) On the other hand, a *contradictory* court order implies (civil procedure) that the aggrieved party is informed of the procedure and is able to discuss the facts and the legal means that the plaintiff is opposing. This means in particular that measures to search for evidence are conducted with the parties and their counsel.

As mentioned in answer to question 17, there is an obligation to hear the aggrieved party before a decision to grant access to the data retained is taken. Thus, the aggrieved party will be informed prior to the access to data retained.

However, in case of administrative and judiciary investigations, there is no requirement to notify the aggrieved party if **this can compromise the efficiency of the investigation** (section 145 of the Code of Civil Procedure). The aggrieved party will be informed so as to be able to challenge the decision of the magistrate in the form of an appeal before the *Chambre de l'Instruction* (Investigative Division) of the Court of Appeal.

Moreover, section 32 of the Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties as amended (French Data Protection Act) states that the data controller shall provide the data subject with the information enumerated in section 32(I) prior to the recording of data or prior to the disclosure of data to a third party. However, section 32 (VI) states that **this obligation of prior notification shall not apply to the processing of data in relation to the prevention, investigation or proof of criminal offences and the prosecution of offenders**.

In other word, there is a general obligation to notify the aggrieved party, except when this may compromise the efficiency of the investigation.

19. Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?

ISPs have to inform their customers on the fact that traffic data will be retained and potentially communicated to legally or judicially authorized persons, but will generally not have to inform the data subjects of a specific communication of data transmitted to judiciary and administrative authorities as the latter are considered as "authorized" third parties*, and this may compromise the efficiency of the measure or of the investigation.

* A definition of the notion of « authorized » third party is provided by Article 3 of the Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties as amended: *« Authorities who are legally entitled to ask the data controller to send them the personal data, in the context of a particular mission or that of the exercise of a right to receive such data »* which means they are allowed to have access to these data under special legislations (police services, magistrates, Independent Administrative Authorities, labour inspectorates etc.).

Moreover, in accordance with sections 60-1, 77-1-1 and 99-3 of the French Code of Criminal Procedure:

- - The judicial police officer - during an inquiry into flagrant crime (*enquête de flagrance*),

- - The public prosecutor or the judicial police officer authorized by the public prosecutor - during a preliminary hearing, and

- - The investigating judge or the judicial police officer committed by him - during the investigation,

may, by any means, require from any person, any institution or private or public body or any government services that may detain documents relevant to the inquiry, including those stemming from a computer system or from a processing of personal data, to hand over these documents.

In other words, the aggrieved party does not have a *right to be informed about the data accessed* per se as far as they are related to him/her.

20. May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?

In case of a non-contradictory request, the aggrieved party will be able to challenge *ex post* the order before the judge who ordered the measure (section 496 of the Code of Civil Procedure) through the fast-track procedure of *référé* (emergency appeal to a judge) dedicated to urgent or obvious matters.

In theory and in order to obtain the annulment of the decision, the aggrieved party has a "*recours pour excès de pouvoir*" (application for judicial review of administrative action) against the decision of the "qualified person" during an administrative request, if the decision is affected for instance by a procedural irregularity or illegality. In case of misconduct by an agent, the aggrieved party can also claim damages before the administration under certain conditions and limitations.

As regards to judiciary request, the aggrieved party may also challenge the decision of the magistrate in the form of an appeal before the *Chambre de l'Instruction* (Investigative Division) of the Court of Appeal.

The aggrieved party can also bring an action against the operators' employee responsible for unlawful data access or processing operation and obtain damages for compensation of its prejudice on the basis of article 1382 of the French Civil code, or if he is a consumer, by way of a contractual liability action against the operator. Compensation may be granted where, for instance, an operator has unduly

communicated data subsequent to an informal request by a police agent, or communicated erroneously data to a third-party.

The aggrieved party may also appeal to a court after the sanction/penalty imposed by HADOPI. There is however no remedy against a decision by HADOPI to simply access retained data.

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

Section L.34-1-1 of the French Posts and Electronic Communications Code provides that the National Commission for Control of Security Interceptions may carry out at any time inspections relating to operations of communication of technical data. When the Commission finds a breach of security obligations, the Commission can report the breach to the Minister of the Interior who will have 15 days to decide what measures shall be taken to remedy any deficiencies found.

Moreover, Article 34 of the French Data Protection Act provides that: "*The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties*". The French Data Protection Authority is entitled to carry out inquiries to monitor the security measures put in place to safeguard personal data, as well as to take administrative sanctions or to refer to judicial authorities.

Failure to comply with the data security requirement or communication of information to unauthorized persons is punishable by a 5-year imprisonment sentence and a 300.000 € fine under section 226-17 of the French Criminal Code.

22. When do the accessing bodies have to destroy the data transmitted to them?

According to section R10-19 of the French Posts and Electronic Communications Code, data provided to police services are recorded and kept for a maximum period of three years in the automated processing implemented by the Ministry of the Interior.

As there is no further detail, this rule shall apply regardless of whether the case has officially been closed or is still being investigated.

Section R10-19 is available at the following URL address (in French): http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1862B61BE241508E51F4EEB1226C6A12.tpdjo03v_3?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006466375&dateTexte=20111228&categorieLien=cid

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

Section 5 of the Act of 23rd of January 2006 has expanded the scope of application of section 34-1 of the French Posts and Electronic Communications Code.

In addition to electronic communications operators and service providers, article L.34-1 of the French Posts and Electronic Communications Code applies to other private bodies or enterprises offer to the public a connection allowing electronic communications through a network access, as a main or secondary activity, for free or not.

In theory, the data retention obligation is applicable as a consequence of activities on a case-by-case basis, and not by way of *ex ante* determination of law. As such, any entity providing to the public a connection allowing electronic communications through a network access is supposed to retain traffic data. Places open to the public offering Internet access to the public are thus required to retain the data: owners of Internet *cafés* or restaurant ("cybercafé"), hotels, airports, on-line gaming centres, post agencies, universities, whether it is by way of wireless connection or access to computers connected to the Internet, either free or for a fee, either as an principal or incidental activity.

However, on the basis of parliamentary debates and documentation drafted as preliminary analysis of the bill (which led to the adoption of the Act of 23rd of January 2006), there seems to be uncertainties, as this section was primarily applicable to cyber-cafés according to some deputies. Yet, this section literally encompasses many other places and the French data protection Authority is often asked by public or private entities whether they are required to retain traffic data.

Internet access offered to employees

The assumption that Internet access is offered by a company or a government to its employees or agents raises the question of data retention. In an opinion of 10 October 2005 on the anti-terrorism bill, the French data protection Authority considered that companies or governments that provide network access are not affected by the data retention obligation, insofar as the connection is only open to their employees or agents.

Nevertheless, in a decision on 4 February 2005, a court of appeal held that a bank should be considered as a technical service provider, because it offered an Internet access to its employees, and thus shall hold and retain data such as to permit the identification of any persons involved in the creation of contents provided by the bank, and shall communicate this data if required by duly authorized authorities.

Host service providers

Host service providers and internet platforms assimilated to host service providers are subject to a data retention obligation under section 6-II of Act n°2004-575 of 21 June 2004 on Trust in the Digital Economy, in order to allow on a case-by-case basis the identification of publishers of illicit content through the IP address.

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

As mentioned in question 23, in theory, all private bodies / enterprises who, as a main occupation or as an incidental one, offer to the public a connection allowing electronic communications through a network access, including for free, are obligated to retain the data.

With regard to host services providers, the application of data retention obligations will depend on the activities in questions. For instance, a search engine with simple website indexing functions will not be considered as providing hosting services. However, if the same search engine offers commercial or advertising links on the result page which content is determined by advertisers, it will be considered as offering ancillary hosting services and will have, for this activity, to retain the data of the advertisers to allow their identification in case, for instance, of intellectual property infringement.

There is no formal request procedure to obtain an exemption from these obligations.

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

See question 1. France Telecom and other network operators were free to retain any categories of traffic data for invoicing purposes or added-value services to which the consumer has consented. But even if there was no limitative enumeration of the categories of data to be collected, such collection of data was subject to the French Data Protection Act N°78-17 which only allows collection of the data which is necessary to the purpose of the data processing. The normalization of the categories of data to be collected did not occurred until the adoption of the decree implementing the Directive.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

Section L.33-1 of the French Posts and Electronic Communications Code provides that the implementation and exploitation of publicly networks, as well as the provision to the public of electronic communications services, must comply with the following rules:

- Permanence, quality and availability of the network and the service;
- Confidentiality and neutrality with regard to the sent messages and information relating to communications;
- Standards and specifications of the network and service.

27. Which *additional* costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate *in total* from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?

Not available.

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

The Act of 23 January 2006 allows Internet service providers to obtain specific financial compensation for costs incurred by operators in case of a request for data communication.

The Decree of 24 March 2006 has established the procedure of such compensation and introduced the section R.213-1 of the French Code of Criminal Procedure, which normalizes the amounts recoverable by operators for the communication of data. The administrative order of 22 August 2006 taken in application of this Decree provides that electronic communications operators will be reimbursed by applying the rates indicated in appendix 1 (e.g.: identifying a subscriber from his phone number – 6,0 €; from his surname, 13€ etc.). For service not included in this appendix, prices will be determined upon estimate.

Costs incurred for the security of retained data are to be borne only by operators as a consequence of their general obligation of security as a data controller under the French Data Protection Act n°78-17 of 6th January 1978 and as part of the implementation of general security measures concerning personal data.

Costs for investments into the required storage technology are not compensated. Operators have tried to challenge the Decree of 24 March 2006 before the *Conseil d'Etat* (French Council of State) in order to obtain compensation for the costs entailed by storage and technology investments without success (see below).

The text of the administrative order of 22 August 2006 taken in application of the Decree of 24 March 2006 is available at the following URL address (in French):

http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=F326F130960332D127958C6C92DA4493.tpdjo04v_3?cidTexte=JORFTEXT000000268186&categorieLien=id

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

With regards to administrative requests, the French Code of Posts and Electronic Communications (Article L34-1-1 created by the Act n°2006-64 of 23 January 2006) provides that requests of access shall be approved by the "qualified person" and only for the purpose of prevention of terrorism, and all communications (internal request, decision of authorisation, request to the operator and transmission of data) must be centralized and controlled by the UCLAT (anti-terrorist agency) and under the *ex post* control of the National Commission of Control of security interception.

Under the decree n° 2007-1538 of 26th of October 2007, judiciary requests shall be approved either by the magistrate in charge of instruction or the magistrate of detention and liberties. The request must be part of an investigation for flagrant infraction, preliminary investigation or "instruction" and only made by authorized officers as part of a public action (indictment by the Public Prosecution Service). A protocol must be signed between the Minister of Justice and, as appropriate, the Minister of the Interior or the Minister of the Budget, and the public or private entity allowing access, detailing the procedure for access and in particular whether the transfer of data is performed by the operator sending a specific file or by a temporary and limited access to the database granted to the officer by the entity. The protocol must also specify the technical conditions ensuring the integrity and confidentiality of data. The access must be documented in a minute

Under the Decree n°2007-1145 of 30th of July 2007, the data collected subsequently to a formal request are stored in a dedicated data processing and transmitted if required by the judges in case of an judicially ordered interception, to the police and customs agents and officers authorized to proceed to investigations. History of accesses and connexions to the system is recorded and the identification and contact details of the recipients of the intercepted data are retained for a period of three years. Some categories of data, especially when content is associated to traffic data, must be encrypted.

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

Section L.39-3 of the French Code of Posts and Electronic Communications provides a one-year imprisonment sentence and a 75.000 € fine (for legal persons, a 375.000 € fine, and a five-year imprisonment sentence (legal representative) – section L.39-10 of the French Code of Posts and Electronic Communications & section 131-38 of the Criminal Code):

- If electronic communications operator or its agents did not carry out processes to erase or render anonymous traffic data in cases where these processes are prescribed by law;

- Electronic communications operator or its agents did not proceed to the retention of technical data under conditions where this retention is required by law.

Natural persons convicted of these offences also incur the prohibition, for a period of five years, to exercise the professional activity during which the offence was committed.

Criminal sanctions regarding the protection of professional secrecy, secrecy of correspondence and more generally data protection are also applicable.

In case of a civil action, an individual may claim damages in case of breach of a legal obligation resulting in an ascertainable prejudice.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

In case of administrative investigations for the prevention of terrorism, only the agent/officer of the UCLAT (anti-terrorist unit) in charge of transmitting the request - after the procedure before the "qualified person" - will be entitled to establishing contact with the operator retaining the data.

In case of judiciary investigations, the police officers in charge of the investigation and authorized by a magistrate will be directly entitled to make contact.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

Not to our knowledge.

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?

See question 30.

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

France has taken the necessary steps to ensure compliance with the Convention on Cybercrime on January 10, 2006 (entered into force in France on May 1, 2006) which provides mutual assistance between States as regards the cross-border communication of traffic data related to criminal offences.

France has signed several bilateral agreements on judicial cooperation in criminal matters (mutual assistance, extradition) applicable to any form of crime, including when the charges involve the use of new communications technologies. In addition, the European Conventions on Mutual Assistance in Criminal Matters (1959) and Extradition (1957) govern judicial cooperation in criminal matters between France and other States that are parties to these Conventions.

Within the EU, cooperation is governed by the instruments adopted within this framework as for instance, the Convention on Mutual Assistance in Criminal Matters of 29 May 2000.

Judicial cooperation in criminal matters is facilitated through a process of harmonization of substantive criminal law leading to the definition of common offences (Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems and Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography). These two instruments also organize, between member states, mechanisms for cooperation and exchange of information relating to offences defined by them, based on the establishment of a network of operational contact points available 24h a day and 7 days a week.

The Central Office of fight against crime linked to information technology and communication (OCLCTIC), created by the Decree of May 15, 2000, is the central point in international exchanges (which means that a direct access of foreign authorities to the data retained by French providers is not legally possible). The OCLCTIC is responsible for all requests (ingoing/outgoing, EU/non-EU countries).

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters sets forth the rules applicable to the transfer of personal data between authorities of the Member-States in charge of investigation and prosecution of crimes.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

CNIL *(Commission nationale de l'informatique et des libertés)*. This Authority's general mission consists in ensuring that the development of information technology remains at the service of citizens and does not breach human identity, human rights, privacy or personal or public liberties. It has a comprehensive supervisory control insofar it also gives many guidelines in terms of technology compliance with law and security requirements. It will have the power to control the data processed by the operators as data controllers.

CNCIS *(Commission nationale de contrôle des interceptions de sécurité)*. This authority may at any time carry out inspections relating to operations of technical data communication. The CNCIS can refer a breach of rules (defined by the French Code of Posts and Electronic Communications) to the Ministry of the Interior. It also controls the decisions of the "qualified person" as regards administrative requests.

CNIL and CNCIS are independent administrative authorities. As such, they are independent from government, but under the supervision of Parliament and the judge. Their independence vis-à-vis the government results from EU texts and the need to distinguish, within the State, between government shareholding and tutelage over companies that are partially or entirely public and the role of neutral regulator vis-à-vis the various operators.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

(i) The Association of Internet Service Providers has brought an action against the Decree of 24 March 2006 before the *Conseil d'Etat* (State Council) in the form of a "*recours pour excès de pouvoir"* (application for judicial review of administrative action), requiring the annulment of the Decree and its application *Arrêté* (administrative order), aiming in particular the provisions related to the compensation of costs incurred by operators for the retention of data.

(ii) Another action has been brought by Members of Parliament before the Constitutional Council challenging the powers conferred to police services in application of the Act n°2006-64 of 23rd January 2006 to request traffic data for operators for the purpose of fight against terrorism.

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

(i) The Association of Internet Service Providers and some Internet Service Providers.

(ii) Members of Parliament

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

(i) Criticism on the lack of clarity and consistency of the decree regarding to the data requested, and failure to take into account the investment costs necessary for the data retention required by law.

(ii) Section 66 of the Constitution that states that none shall be detained arbitrarily and that the judicial authority, guardian of individual liberties, ensures the respect of the principles as provided by law.

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

(i) The *Conseil d'Etat* dismissed the action on 7 August 2007, validating most of the compensation framework, except for the provision concerning compensation "on quote", the *Conseil d'Etat* considering that the amount should be set in advance).

In its first decision regarding the annulment of the Decree, the *Conseil d'Etat* considered that the Decree distinguishes sufficiently clearly and precisely categories of data to be retained et those to be deleted. The *Conseil d'Etat* also considered that the Decree does not affect privacy right disproportionately as compared to the purpose of public safety.

In its second decision regarding the Order of 22 August 2006, the *Conseil d'Etat* did not challenge the government's choice regarding the costs reimbursement. However, the *Conseil d'Etat* cancelled the table annexed to the Order (containing the reimbursement rates for mobile and fixed operators) considered as unlawful.

(ii) In its decision n°2005-532 of 19th January 2006, the *Constitutional Council* has validated the powers conferred to police services in application of the Act n°2006-

64 of 23rd January 2006 to request traffic data for operators for the purpose of fight against terrorism, considering that:

- *"Section 66 of the Constitution which states that "none shall be detained arbitrarily and the judicial authority, guardian of individual liberties ensure the respect of the principles as provided by law" is not breached by a provision which merely establishes a procedure of requisition of technical data";*

- *-"The legislator must ensure the conciliation of, on the one hand, the prevention of public order violations needed to safeguard the rights and principles of constitutional values, and on the other hand, the exercise of liberty as constitutionally guaranteed, such as respect of private life and freedom of enterprise, as protected by articles 2 and 4 of the Declaration of the Human and Citizen rights of 1789";*

- *- "In this case, the legislative has associated the procedure of requisition of technical data with the proper limitations and precautions in order to ensure the conciliation of the private life of the persons, the freedom of enterprise of operators and the prevention of terrorists acts."*

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

Not to our knowledge

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

Electronic communication service providers are free to decide the modalities of storage of the data retained. The current trend is to outsource data storage in countries like India, Morocco, US etc. Big providers practices are no exception.

Insofar as the data processing includes personal data, the third-party data processor should be mentioned in the declaration before the French data protection authority if applicable. The location of the "exploitation" of the data should also be mentioned, which can cover the notion of storage of data.

The data stored as a result of a request for access by habilitated police services as part of investigation on terrorism are stored at Levallois-Perret in Paris Region in a centralized information system of the UCLAT.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

As regard ISPs and other electronic communications networks and services, the data storage can be outsourced outside French territory subject to the restrictions applicable to transfers of personal data outside the European Union.

The French Data Protection Act 1978-17 of 6 January 1978 as amended by the Act of 6 August 2004 prohibits the transfer of personal data from France to any entity (either service provider premises or external companies) based in a country outside of the European Economic Area (EEA), whose laws do not provide an adequate level of protection for the transferred data.

The service provider may transfer the data to a State not satisfying these conditions if the data subject has expressly consented to this transfer or if the transfer is necessary subject to one of the following conditions for:

1. the protection of the data subject's life;

2. the protection of the public interest;

3. the meeting of obligations ensuring the establishment, exercise or defence of legal claims;

4. the consultation, in accordance with legal conditions, of a public register that, according to legislative and regulatory provisions, is intended for public information and is open for public consultation or by any person demonstrating a legitimate interest;

5. the performance of a contract between the data controller and the data subject, or of pre-contractual measures taken in response to the data subject's request;

6. the conclusion or performance of a contract, either concluded or to be concluded, in the interest of the data subject between the data controller and a third party.

There may also be an exception to this prohibition by a decision of the French Data Protection Authority (CNIL) where the processing guarantees a sufficient level of protection of individuals' privacy as well as their liberties and fundamental rights, particularly on account of contractual clauses or internal rules relating to the processing.

Data processors and hosts are generally subject to an obligation of security and confidentiality, i.e. implementing the measures of useful precautions with regard to the nature of data and risks inherent to the data processing, so as to preserve the security of the data and prevent their alteration or unauthorized access.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

c) data are not used for purposes other than those they are permitted to be used?

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

e) data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?

f) the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?

g) sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?

As a general observation, technical and organisation measures are not strictly normalized from a legal standpoint, as any prescription would be deemed to be invalid with the fast evolving nature of technology and security standards.

Yet, companies have to be able to justify the technical and/or organisational measures taken to implement section L33-1 of the French Post and Telecommunications Code ex post in case of controls of the *ARCEP*, the French Telecommunication and Posts Regulator. However, there is no need to justify the measures implemented ex ante via the system of prior declaration to the ARCEP that operators are subject to.

Moreover, companies have to be able to justify the implemented security measures – (via for instance the adoption of an IT security policy), ex ante via the declaration to the data protection authority if applicable (essentially in case a prior authorization from the DP Authority is necessary) and ex post in case of controls. Nevertheless, the description of the technical and organisational security measures implemented required by DP Authority do not necessarily include all measures taken to implement section L33-1 of the French Post and Telecommunications Code.

Yet, the French data protection Authority (CNIL) has recently (7 October 2010) released a guide on personal data security. This guide is intended to help data controllers to comply with their obligations regarding personal data security and is inspired by international norms of data security.

This guide contains 17 memos including the following themes: security risks, user authentication, Management of access, Backup, Maintenance, premises safety, network security, archives, the exchange of information with other agencies, IT development, encryption etc. Each memo is divided into three sections: (i) basic precautions, (ii) what not to do, (iii) to go further.

Among all recommendations, some are good practices on management of information systems security, while others result from the rules on personal data protection.

This guide is available at the following URL address (in French):
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf

To our knowledge, there is no "privacy-by-design" measure as regards the information systems of the ISPs.

However, the information system of the UCLAT centralizing the data obtained as a result of a request by the police service provides for encryption of the data for communication purposes and secured access to authorized agents.

41. Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?

The CNIL supervises compliance with the law, by inspecting IT systems and applications. The Commission uses its inspection and investigation powers to investigate complaints, improve its knowledge of some specific files, better appreciate the implications of using IT in some sectors, and following up on its deliberations.

The CNIL also monitors the security of information systems by checking that all precautions are taken to prevent the data from being distorted or disclosed to unauthorized parties.

The CNIL may pronounce different types of sanctions: warnings, injunctions, financial sanctions up to €300.000, orders to stop processing operations. The Chairman may also file a petition in court to order any necessary measure. He can, on behalf of the Commission, report breaches of the law to the Prosecutor.

Audits or Chief privacy Officers are optional in France.

42. What technical (*de facto* and/or *de iure*) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?

No information available.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

Administrative request procedure:

1st step: If access to communication data is needed within an intelligence inquiry, the competent agent among the 551 authorized agents from the services in charge of prevention of terrorism (whose list is fixed by administrative order of 31 mars 2006) may send a request by electronic encrypted e-mail to the UCLAT (counter terrorist unit). The UCLAT operates a technical platform to centralize the requests. The requests must contain the information on the identity of the person who requested the data, the precise nature of the data requested and the motive for the request. The UCLAT then examines the request, verifies the identity of the requestor and all justifying papers.

2nd step: The UCLAT transmits the demand to the "qualified person" who examines the request generally within the day and takes a binding decision of refusal or approval or can ask for further details before reaching a decision.

3rd step: The decision is transmitted to the UCLAT. In case of approval, the UCLAT will directly ask the operators to push the data generally within 24 hours.

4th step: The data requests will be transmitted from the operators to the technical platform of the UCLAT, so as to ensure their security integrity subject to a convention or administrative order. If there is no convention or order, the operators will transmit the data with the modality they choose, which will generally not correspond to the information technology standards of the police, who will thus not be able to exploit them in an optimal way (obligation to integrate manually the data) (to our knowledge, there is no more details on the level of data security in case there is no convention or administrative order). A project of administrative order should impose the XML standard.

5th step: The UCLAT will then transmit the data to the service of the person who requested the data, who will be able then to use them as specified in the request. The decree 22nd of December 2006 (R 10-19 CPCE) provides that the data must be retained and stored for a maximum of three years into the database processed by the ministry of the Interior.

Lastly, section R. 10-20 of the French Code of Posts and Electronic Communication provides that the requests approved by the qualified person are transmitted within 7 days to the CNCIS, in compliance with the modalities of the administrative order of 10 may 2007 of the Ministry of the Interior.

As regards judiciary requests, the communications between the officer and the operators are theoretically formalized in protocol taken by the Minister of Justice and, as appropriate, the Minister of the Interior or the Minister of the Budget with the concerned entity.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

See question 34.

In civil and commercial matters for instance, cross-border requests are issued or responded to according to the Hague Convention (March 18, 1970) on the taking of evidence abroad in civil and commercial matters and/or the Council Regulation n°1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

These two texts apply in civil and commercial matters where the court of a country requests the competent court of another country to take evidence, or requests that evidence be taken directly in another country.

The Regulation lays down that requests must be drafted in the official language of the Member State of the requested court or in any other language that the requested Member State has indicates it can accept.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

The French Law on Data Protection enacted in 1978 was at the time subsequent to a public debate entailed by the revealing, by the media, of the implementation of a file called SAFARI supposed to be a comprehensive mass-profiling database of French citizens.

French citizen are still aware of the risks of mass-surveillance: the 27th June 2008, a decree 2008-632 was adopted by the right-wing government to create the file EDVIGE, a centralization of several databases held by different intelligence agencies about to merge. The scope and modalities of implementation of this database was harshly criticized by numerous parties including the left-wing and socialists, green parties, democrats, and some personalities of the right-wing party. Twelve major trade unions and associations including for instance the League of Human Right brought an action before the *Conseil d'Etat* in order to obtain the annulment of the decree. This issue has had tremendous impact in the media with public street gathering and a petition of 215.000 signatures against the EDVIGE database. The government eventually retracted in November 2008 and changed some of the criticized provisions.

Yet, there is still a quasi-consensus among citizens on the generalization of surveillance CCTV, the right-wing government using public security as a leitmotiv and priority to its general policy. Because of some shortcomings, popularity/credibility of the right-wing party on its public security policy is challenged in many aspects.

There also has been a lot of public debate surrounding the enactment of the HADOPI law on copyright allowing the surveillance of Peer-to-Peer networks, the identification of IP addresses justifying a request for access to electronic communication operators.

Public debate on data retention has been also under the lights of the media in November 2010. A tax privilege story involving members of the government led the Ministry of the Interior to proceed to investigations on the relations between a journalist and a public officer, supposed to be the source of the revelation of the story. To identify the relations between those two, the intelligence agency requested access to communication data to operators i.e. allegedly using the administrative request procedure, whereas such procedure is limited to prevention of terrorism. It raised a public debate and a lot of media attention on the protection of the source of journalist and the legality of the procedure used by the government agencies to obtain communication data.

46. Are there any obligations in your country to retain other personal data without a *specific* reason (e.g. passenger name records (PNRs), employment data, etc)?

In theory, French law on data protection prohibits the collection of data unless it is linked to a legitimate, explicit and determined purpose (section 6-2° of the Act 78-17 of 6th January 1978). As a consequence, there should not be collection or retention of data without a specific purpose.

However, there are some obligations to retain personal data without a *specific* reason, for the "prevention" of terrorism:

- Resulting from bilateral agreement, such as the retention of PNR, SWIFT data,

- Resulting from national legislation, such as the retention of video surveillance data.

There are also obligations to retain personal data for the fight against money laundering and against financing of terrorism.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

There are general statistics on the number of requests by categories in particular by the Commission in charge of a *ex post* control of administrative requests and judicial requests but, to our knowledge, no feedback on how the access to data helped resolving or preventing a crime.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

Not available to our knowledge.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

We are still waiting for a decree to be taken in application of the Act n°2004-575 of 21 June 2004 on Confidence in the Digital Economy in order to determine precisely the categories of data to be retained, as well as the categories of private bodies/enterprises obligated to retain the data.

The 3rd of May 2010, Jean-Louis MASSON a French senator proposed a bill to facilitate the identification of editors of blogs, and the 9th of November 2010 the senators Yves DÉTRAIGNE et Anne-Marie ESCOFFIER proposed a bill aiming to better preserve privacy in the digital era and providing an obligation for data controller to inform the data subject on the period of retention of the data. A new bill on cyber-security (LOPPSI) is also being prepared giving more powers to police services to retrieve data directly from computers of individuals suspected of a crime.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of

thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law1 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The right of privacy is not explicitly included in the French Constitution of 1958, but the Constitutional Court rules in 1995 that the right of privacy was implicit in the Constitution (especially under article 66 the Constitution which states that none should be detained arbitrarily and that the judiciary authority is guardian of the individual liberties).

More specifically, article 9 of the French Civil Code, inserted by Act of 17 July 1970, provides that "*everyone has the right to respect for his or her private life*".

The French data protection Act 1978-17 of 6 January 1978 as amended by the Act of 6 August 2004 protects personal information held by government agencies, private bodies / enterprises.

The Act n°91-646 of 10 July 1991 relating to secrecy of correspondence sent through electronic communications states that "*the secrecy of correspondence sent through electronic communications is guaranteed by law*". According to the Act of 10 July 1991 relating to secrecy of correspondence, and conformingly to article 100 to 100-7 of the Code of Criminal Procedure, the secret can be waived by public authority only in cases of public interest necessity as required by law and within the limits set by it (interceptions ordered by judicial authority or security interceptions).

Moreover, the Declaration of the Rights of Man and of the Citizen, of constitutional value, grants to citizens several rights such as freedom of expression and information, freedom of thought, religion, conscience, etc.

Pursuant to the 2005 decision of the Constitutional Council on data retention, apart from the right to security and the right to privacy, freedom of enterprise is also concerned as data retention imposes an obligation - with related costs - to electronic communication operators and others entities. Such costs might also entail distortions of competition between operators, which justifies a fair compensation.

More generally, data retention obligation affects many of the constitutional rights and individual liberties:

---

[1] In the following, „national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

(i) The separation of powers between the executive and the judiciary powers and the checks and balance to ensure that request for access of data are properly motivated and stands as a proportionate measure to a legitimate purpose;

(ii) The right to due process and law of evidence as regards technical data as admissible proof before the jurisdictions;

(iii) Freedom of expression and opinion, and freedom of the press, as regards the retention of data required to identify the author of content published on the Internet, where anonymity is considered as a safeguard allowing free expression without fear of repression.

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

Limitations to fundamental rights generally comply with the criteria of the European Convention of Human Rights where restrictions must stand as a necessary measure in a democratic society to ensure legitimate interests such as public security, public health, prevention of crimes and individuals rights of others.

Depending on the right at stake, there may be explicit limitations. For instance, section 222-17 of the Criminal Code prohibits the threat to commit a crime against individuals. Section 223-14 prohibits advertising in favour of methods of suicide or infringement to professional secrecy. Section 23 of the Act of 29th of July 1881 on freedom of the press prohibits the incitation to commit a crime and section 29 prohibits defamation or insults. Notwithstanding, the general notion of abuse of right may also be used by the courts to limit the freedom of expression of employees for instance on a case-by-case basis.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

In its decision n°2005-532 of 19th January 2006, the Constitutional Council has validated the powers conferred to police services in application of the Act n°2006-64 of 23rd January 2006 to request traffic data for operators for the purpose of fight against terrorism, and gave a general opinion on the conciliation, through adequate safeguards, of the requisition of technical data for the prevention of public order violations with liberties constitutionally guaranteed such as the respect of privacy:

"(i) Section 66 of the Constitution which states that "none shall be detained arbitrarily and the judicial authority, guardian of individual liberties ensure the respect of the principles as provided by law" is not breached by a provision which merely establishes a procedure of requisition of technical data;

(ii) The legislator must ensure the conciliation of, on the one hand, the prevention of public order violations needed to safeguard the rights and principles of constitutional values, and on the other hand, the exercise of liberty as constitutionally guaranteed, such as respect of private life and freedom of enterprise, as protected by articles 2 and 4 of the Declaration of the Human and Citizen rights of 1789;

(iii) In this case, the legislative has associated the procedure of requisition of technical data with the proper limitations and precautions in order to ensure the conciliation of the private life of the persons, the freedom of enterprise of operators and the prevention of terrorists acts."

53. Does national (constitutional) law safeguard an *absolute* limit as to the maximum degree to which public surveillance measures *collectively* may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

The balance of interests has to be carried out in each individual case insofar as the main criteria for control are assessing the proportionality and necessity of the surveillance measures with regard to the objective to be achieved.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

There is a clear distinction between traffic data and content data, which as a general rule cannot be retained and can be recorded only in specific situations and conformingly to the Code of Criminal Procedure, section 100 to 100-7. Content data, as opposed to traffic data, is subject to more stringent procedure and control, and cannot be retained unless authorized by a magistrate.

Moreover, a specific framework is provided for as regards the retention of geo-localisation data in the French Posts and Electronic Communications Code (in addition to the provisions related to the retention of data for purposes of crime research, finding and prosecution; as well as for billing and payment purposes (see answer to question 9):

- Geo-localisation data can be used during the communication only for delivery purposes;

- Geo-localisation data can be held and processed after the completion of the communication (and thus for the provision added-value services) only with the consent of the subscriber (section L.34-1-IV).

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your

opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

In its decision n°2005-532 of 19th January 2006, the Constitutional Council has considered that the legislative has associated the procedure of requisition of technical data with the proper limitations and precautions in order to ensure the conciliation of the private life of the individuals, the freedom of enterprise of operators and the prevention of terrorists' acts.

The data retention obligation entails costs supported by the operators, which restrict their freedom to determine the business method that best suits their objective and the allocation of their investments. As such, the compensation mechanism, limited to costs incumbent to the transmission of the data has been considered by the Constitutional Council as satisfying to ensure the balance of interests.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

In theory, the prevention of crimes is a privilege of the administrative police law and enforcement of the judiciary police. For instance, the Constitutional council recently overruled a new a particular section of the French bill on homeland security that allowed private actors to implement CCTV systems on behalf of public authorities, the constitutional council considering that only the administrative police is in position of ensuring the adequate balance between security requirements and individual liberties (Constitutional Council, 10 march 2011 - decision n° 2011-625 DC).

Moreover, private security activities are regulated professions in France since the Act of 12th of July 1983, n°83-629, which provides an obligation for professionals to obtain a prior administrative authorization ("*agrément*"). Private security agents must justify of professional aptitude and education conformingly to Act 2003-239 of 18th March 2003 and obtain a professional card conformingly to the decree n° 2009-137 of 9th February 2009. These activities are subject to a general framework with obligations of identification, secrecy, limitation of intervention to private place (...) and in particular, prohibition to create personal databases.

With the increase by 3% per year of the numbers of agents of private security who will be 200.000 by 2014, the French government is seeking to create a national council aimed at harmonizing the deontology of the profession, the authorization procedure and the disciplinary sanctions.

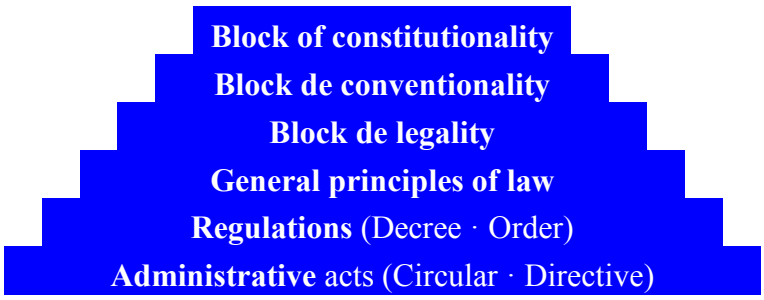
57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

A principle of financial compensation for costs incurred by operators is provided by the Act of 23 January 2006 that provides a reimbursement for identifiable and specific additional costs born from requests of data communication and the delay of anonymisation process, but this is not derived from constitutional norms.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

Hierarchy of norms in France



In a decision of 30 October 1998, *Sarran, Levacher et autres*, the *Conseil d'Etat* considered that "*supremacy conferred to international undertakings by section 55 of the Constitution do not apply to provisions of a constitutional nature*", meaning that the French Constitution has higher value in the hierarchy of norms than International law, notwithstanding the possibility of changing the Constitution so as to ensure its compatibility with an international convention.

Thus, national law implementing international treaties and agreements are considered to be at a higher level than other national law, except constitutional law.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

Since a decision by the *Conseil d'Etat* of 30 October 2009, any individual can rely, in support of an action against an administrative non-regulatory act, on the precise and unconditional provisions of a directive, when the Member-state has not taken the necessary transposition measures on time.

European directives can be implemented into French law either by statutes or by regulations. It also happens that the transposition of a directive is made partly by law and partly by way of regulation (decree or order).

The implementation of a European directive into French law has to comply with the hierarchy of norms and the distribution of matters between legislation and regulation. In order to determine if provisions of the Directive to be transposed have to be dealt with by legislation or by regulation, the following questions must be answered:

- First, what are the provisions of the Directive to be transposed;

- Second, what are the norms existing in French law that already transpose some dispositions of the Directive;

- Third, what is the legal nature of the new norms that have to be adopted in order to ensure an entire transposition of the Directive.

Then, a proposal of the legal text to be adopted is made.

In a decision of 10 June 2004 about the Act on Trust in Digital Economy (LCEN), the Constitutional Council considered that the transposition into national law of EU Directive results from a constitutional requirement, which could be blocked only for breach of "express" provision of the Constitution. But there is no definition of "express" provision.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

In France, transfers of sovereignties are prohibited, but limitations to this sovereignty are authorized (preamble of the French Constitution of 1946). Transfers of competences are allowed under the condition that they do not affect "essential conditions of exercising national sovereignty".

Under article 88-2 of the Constitution, transfers of competences can only occur:

(i) For the matters listed in article 88-2, and in particular economic and monetary union, external boundaries, free movement of persons, and the European arrest warrant – if needed in case of a transfer of sovereignties by an international treaty, a prior revision of the Constitution will be done to ensure their is no incompatibility;

(ii) Under condition of reciprocity from other Member-States;

(iii) Subject to the conditions set forth by the European treaties;

(iv) Subject to the authorization by the Parliament and a ratification Act pursuant to article 11 of the Constitution.

However, the entry into force of the Lisbon Treaty on the functioning of the European Union has substantially modified the formulation, content and scope of these provisions, so that the notion of common exercise of competences is now the basis for the determination of sovereignties.

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

The powers to access to data have been divided between:

(i) The administrative police in charge of prevention of crimes, with regards to the prevention of terrorism, under the Authority of the Prime Minister;

(ii) The judiciary police in charge of investigations and repression of crimes under the authority of the Minister of the Interior and controlled by the judiciary authorities;

(iii) The HADOPI (independent authority for the diffusion of works and protection of rights) who has the power to request from the electronic communication service providers the identifying data required in order to investigate on copyright infringement pursuant to the complaint of a copyright holders, under section L. 331-21 of the Code Intellectual Property and L. 34-1 of the Code of Posts and Electronic Communication.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

Data subject (consumers of ISPs for instance) should be informed of the recipients of the data, including where those recipients are located in a foreign country. These recipients should be mentioned in the notification to the Data Protection Authority if applicable*.

* For instance, if the processing benefits from an exemption of notification, the company will not have to declare to the DP authority the recipients. However, in case of a mere notification to or a prior authorization from the DP Authority, the company will have to mention the recipients and the countries in which they are established in case they are located outside the EU

If those recipients are located outside the European Union, traffic data retained by electronic communication cannot be transferred unless these countries offer an adequate level of protection through the implementation of Binding Corporate Rules

or Standard Contractual Clauses, adhesion to Safe Harbor Principles in the U.S. or pertaining to Commission's decision of adequacy.

Transfer outside the EU can also be executed if the data subject has given explicit consent or by application of one of the 6 exemptions provided by section 69 of Act 78-17 of 6th of January 1978.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

(i) Data subjects should be more clearly informed on the period of retention of the data by data controllers;

(ii) A procedure of habilitation/authorization for the operators' employees in charge of transmitting the data to the police services;

(iii) The CNCIS should be able to control ex post the qualified person's decision when it is a refusal;

(iv) France still needs to take a decree concerning the data retention obligation of host services operators.

Appendix 1

Reimbursement for costs (question 28)

http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20060901&numTexte=16&pageDebut=13010&pageFin=13012