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

Luxembourg

*Prof. Dr. Mark D. Cole / Dr. Franziska Boehm**

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

Key terms / abbreviations for laws used in the questionnaire:
CNPD: Commission Nationale de la protection des données / National data protection commission
Loi 2005: Loi du 30 mai 2005 – relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et – portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle[1]
amended by
Loi du 27 juillet 2007 portant modification – de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; – des articles 4 paragraphe (3) lettre d); 5 paragraphe (1) lettre a); 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et – de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias[2]
and the

* The author *Cole* is Associate Professor for the Law of the New Information Technologies, Media and Communications law at the University of Luxembourg (www.medialaw.lu), the author *Boehm* is research associate at the University's Interdisciplinary Centre for Security, Reliability and Trust (SnT).

1 Mémorial A, no. 73 from 7 June 2005, p. 1168.

2 Mémorial A, no. 131 from 8 August 2007, p. 2330.

Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle[3]

In the following text reference is always made to the Loi 2005 in the version of the last amendment of 2010 except were expressly noted differently.

Règlement 2010: Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics[4]

Loi 2002: Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (General Data Protection Act of Luxembourg)[5]

last amended by the

Loi du 27 juillet 2007 portant modification – de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; – des articles 4 paragraphe (3) lettre d); 5 paragraphe (1) lettre a); 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et – de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias[6]

In the following text reference is always made to the Loi 2002 in the version of the last amendment of 2007 after which an official consolidated version ("version coordonnée") was published, accessible at: http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf#pagemode=none.

CIC: Code d`instruction criminelle/Criminal Procedure Act,

accessible at: http://www.legilux.public.lu/leg/textescoordonnes/codes/index.html

CP: Code pénal luxembourgeois/ Luxembourgish Criminal Code,

accessible at: http://www.legilux.public.lu/leg/textescoordonnes/codes/index.html

Juge d'instruction: Investigative Judge (judge who leads the investigation)

For the key laws concerning data protection in electronic communications, unofficial English translations are available. These will be used irrespective

[3] Mémorial A, no. 122 from 29 July 2010, pp. 2060.

[4] Mémorial A, no. 122 from 29 July 2010, pp. 2061.

[5] Mémorial A, no. 91 from 18 August 2002, p. 1836.

[6] Mémorial A, no. 131 from 8 August 2007, pp. 2330.

of the wording applied in the translation. In cases of doubt the original French versions should be consulted via the links provided or generally under www.legilux.lu.

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 Loi 2005 by the amendment enacted with the law of 2010 and the executing Règlement 2010 based on the afore mentioned law transposed the Directive's provisions into national law.

The Loi 2005 in its original version had already allowed for data retention for a one year period, but did not entail a list comparable to the Règlement 2010 which enumerates the data categories allowed to be stored. The act was part of the « Paquet telecom 2005» and transposed Directive 2002/58 into national law. An amendement in 2007 reduced, among other points, the retention time period from twelve to six months.

- ***If transposition has not at all, or only in parts, 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)?

Not applicable.

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?**

   Not applicable.

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.**

   Not applicable.

- ***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.**

   For the Loi 2005 in the version of 2007 an unofficial translation in English language exists for working purposes (unofficial translation accessible at: http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi30052005_en.pdf).

   Not yet considered in this version are the changes of 2010. In the near future the University of Luxembourg might commission a translation of those amendments as well as the Règlement 2010 which would then be published with all other English translations of relevant laws at: www.medialaw.lu.

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

   The changes in 2010 entered into force the first day after the publication in the "Mémorial", which means on the 30th July 2010.

   The Loi 2005 in the original version already allowed for data retention but did not entail a list of data to be stored comparable to the Règlement 2010 which enumerates the data categories allowed to be stored. That law had entered into force on 1st July 2005.

   There are no transition periods in place.

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**

   Act of Parliament (Loi 2005) and an executing regulation (Règlement 2010) which contains a list with the data categories to be stored (equivalent to the list of the Directive).

   The Règlement 2010 is limited to some definitions and a list of data concerned by the obligation to store. The Loi 2005 regulates mainly the following points: obligation to store data for the purpose of prosecution of crimes for a fixed time period; the general description of the data to be retained and an authorisation to regulate this more precisely in a Règlement; the protection of the data against unauthorized access; security measurements; gathering of statistical information.

   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**

      The Règlement 2010 corresponds to an executing regulation and enumerates only the data categories allowed to be stored as well as a few definitions; all main points are contained in the Loi 2005.

   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.**

      The types correspond to those usually chosen in Luxembourg. It is normal procedure to have a law for the main points and one or several executing regulation(s).

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 terms of article 2 para 2 (a) and (c)-(f) Directive 2006/24 are defined in the same terms as in the Directive in the Règlement 2010.

   The term "user/utilisateur" is defined in the Loi 2005 and differs only slightly when comparing it to the Directive. According to article 2 (m) Loi 2005, a user is not only a person who is using a publicly available electronic communications service, but

also a person who is demanding a publicly available electronic communications service.

Art. 2 of Loi 2005 in the original (and in that respect still valid) version defines further key terms from the electronic communications networks and services package, such as "electronic communications network", in line with the provisions from the Directives.

In conclusion, the definitions laid down in these Directives (2002/21/EC and 2002/58/EC) and those laid down in the Loi 2005 are identical and have been transposed correctly, including the previous directives (95/46/EC), however, evidently, partly in/by other laws.

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?**

   There are no additional retention obligations. The list exactly corresponds to the data categories listed in article 5 of the Directive and does not go beyond these requirements. It refers to traffic data and location data (compare Art. 3 Règlement 2010).

   Articles 5 (1) (a) and 9 (1) (a) Loi 2005 entail the obligation to store data on unsuccessful call attempts following the example of article 3 (2) of the Directive (same wording).

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.**

    With consent of the user there is the possibility of listening, taping or storing of the communication or the related traffic data according to Art. 4 para. 2 of Loi 2005. However, this provision does not preclude the storing of data necessary for the functioning of the electronic communications network (cf. esp. Art. 4 para. 3 a)). In addition, Art. 5 para. 3 explicitly allows processing of traffic data necessary for billing purposes, but only to the maximum extent of the time that such a bill can be challenged and at max. 6 months if the bill has been settled undisputedly. A further possibility concerns location data (other than traffic data), which can be processed according to Art. 9 para. 3 even without consent if it is in anonymous form (but after information if the user and with the possibility of withdrawal of consent if that had been given upon information) and to the extent needed to provide the value added service.

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

Data are retained in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of criminal offences, which can be punished with a maximum sentence of one year or more according to Article 5 (1) (a) and Article 9 (1) (a) Loi 2005.

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)?

There are no specific rules in the act transposing the Directive (Loi 2005).

Articles 88-2 and 88-4 CIC however protect the communication of persons underlying the professional secrecy and persons not suspected of having committed a crime or having participated in a crime. The recording or transcription of such data must be immediately destroyed by the juge d'instruction or the person in charge of the secret service and may not be used in criminal proceedings.

Article 6 Loi 2002 refers to the processing of specific categories of 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, including the processing of genetic data. Their processing is generally forbidden. Exceptions exist in several cases, among others if the processing is implemented in the context of processing of legal data for the purpose of criminal investigations and legal proceedings specified in the CIC, in the Civil Procedure Code[7], the Act relating to Procedural Rules before Administrative Courts[8] or other laws (Article 6 (2) (i) in connection with Article 8 (1) of the Loi 2002.

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 therefore.

All of the data have to be retained six months according to article Article 5 (1) and Article 9 (1) (a) Loi 2005.

---

7 Nouveau Code de procédure civile (3 août 1998), Mémorial A, no. 64 from 17 August 1998, last modified by Loi du 5 juin 2009, Mémorial A, no. 134 from 15 June 2009, p. 1889, accessible at: http://www.legilux.public.lu/leg/textescoordonnes/codes/index.html.

8 Loi du 21 juin 1999 portant réglement de procédure devant les juridictions administratives, Mémorial A, no. 98 from 26 July 1999 last modified by Loi du 28 July 2000, Mémorial A no. 71 from 9 August 2000; accessible at: http://www.legilux.public.lu/leg/a/archives/1999/0098/a098.pdf #page=2

The Loi 2005 initially provided for a storage period of 12 months. It was amended in 2007 already reducing the retention period to 6 months as it is now upheld by the amendment of 2010. There was political consensus about the need to restrict the length of retention.

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)?

According to Article 5 (1) (a) and Article 9 (1) (a) Loi 2005, only "autorités judiciaire" (judicial authorities) are entitled to access. Article 5 (2) Loi 2005 refers to the judicial authorities mentioned in Article 67-1 and 88-1 to 88-4 CIC. These provisions deal with confiscation (Art. 67-1) and surveillance measures (Art. 88-1 to 88-4) and in doing so refer to the responsible authorities.

The reference to CIC at this point only serves to mention the authorities concerned since these are not defined within the specific laws, but they refer to the list in the CIC. The actual basis for access to stored information does not derive itself from the CIC but the Loi 2005.

Articles 67-1 and 88-1 CIC mention the juge d'instruction. In addition to acting himself he can also delegate the investigative action to the police according to Article 52-1 CIC.

Article 88-2 CIC refers to the juge d'instruction as well as to the president of the judges' chambers of the court of appeals.

Articles 88-3 to 88-4 CIC additionally mention the Prime Minister who can also demand access to the data retained for the use of the secret service. Again, this is only to show the different possible categories of accessing authorities and in this context the access by the Prime Minister for the purpose mentioned falls within one of the categories (without thereby defining its activities as "judicial", but they are mentioned as one of these authorities). On the other hand it should be mentioned that access by secret service is not deemed to be a "normal" occurrence but the absolute exception.

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)?

The purpose is not specified more precisely. Data are retained in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of criminal offences, which entail a maximum sentence of at least one year according to Article 5 (1) (a) and Article 9 (1) (a) Loi 2005.

After a permission of the judicial authorities mentioned in question 14, the data can be used in order to safeguard the security of the state, the defence, public security and for the prevention, investigation and detection and prosecution of criminal offences (Article 5 (2) Loi 2005). In that way data accessed turns into "judicial data" as specifically regulated in Art. 8 Loi 2002, and in consequence is also treated as such, i.e. like any criminal procedure file.

There is no right for individuals to access the data retained directly.

The data may however be "requested by the competent bodies with a view to settling disputes, in particular interconnection or billing disputes" (Article 5 (2) Loi 2005). In addition to such disputes there is a potential field of use of the data in connection with disputes concerning violation of intellectual property rights. The latest amendment to the Intellectual Property law in 2009[9] introduces in transposition of Directive 2004/48/EC the possibility to request data in civil procedures if necessary to support the claim. However, there is no direct link to the data retained fulfilling the requirements of Loi 2005 because the bodies that have the competence to request are limited. However, it is possible that a court orders information to be given to the plaintiff and this information might be taken by the provider from the retained data. As of now it is not clear to what extent Luxembourgish courts will interpret this new procedural safeguard.

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)?

It has to be a crime that can be punished with a maximum sentence of one year or more according to Article 5 (1) (a) and Article 9 (1) (a) Loi 2005 and a previous court order demanding access to the data according to Article 5 (2) Loi 2005 and referring to Article 67-1, 88-1 to 88-4 CIC has to exist.

Therefore, serious crimes committed by natural persons can fall under this scope. Examples are:

- Crimes against state security according to Art. 113 et seq. CP
- Terrorism according to Art. 135-1 et seq. CP
- "Ordinary" crimes such as murder, rape etc. (crime de droit commun) which are punished by penalties foreseen in article 7 to 13 CP as long as this surpasses at least one year of maximum sentence
- the same applies for offences which do not fall into the category of crimes but also have the same time-limits for imprisonment, such as robbery (including use of violence) which is punished by a minimum 5 year-imprisonment according to Art. 468 et seq. CP

[9] Loi du 22 may 2009, Mémorial A, no. 117 from 28 May 2009, accessible at: http://www.legilux.public.lu/leg/a/archives/2009/0117/a117.pdf#page=2.

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?

It is required to obtain a previous judiciary permission by the judicial authorities according to Article 5 (2) Loi 2005 (judicial authorities refers the authorities listed in Article 67-1, 88-1 to 88-4 CIC), see above question 16.

The aggrieved party is not to be heard or involved. Article 67-1 (3) code of criminal procedure, however, provides for the obligation to subsequently inform a person concerned about the data use not later than 12 months after the access was ordered, if a measure according to Article 67-1 CIC has taken place. The information obligation derives from the criminal procedure law and is regulated in Article 67-1 CIC concerning confiscation and in a similar fashion in Art. 88-2 para. 6 for special surveillance measures during which the telecommunication activity of a person is monitored with an obligation to inform that person no later than 12 months following the end of the surveillance measure. However, to underline it again, Art. 5 (2) Loi 2005 simply refers to the obligation of the providers to grant access to the judicial authorities if they are active in a procedure according to the abovementioned articles from which the obligation of these authorities derives to respect certain procedural rules in view of the concerned individual.

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?

The law transposing the Directive remains silent on this issue. However, there is a notification procedure foreseen in the CIC as described in question 17.

Possible derogations from the 12 month time limit to notify after date of access in Article 67-1 (3) CIC are: the access order refers to a case involving a criminal association or organisation, it is related to terrorism or concerns the sale of medical substances or the fight against "toxicomanie" ("War against drugs").

In addition one can mention the general obligation to inform about the retention of data: The Loi 2002 provides for a notification duty "when the data are collected directly from the data subject, the controller must supply the data subject, no later than the point at which the data are collected …".[10] However, this information duty shall not apply when the processing is, among others, necessary to safeguard national security, defence, public safety or the prevention, tracking down, recording and prosecution of criminal offences, including the combating of money laundering, the progress of other legal proceedings, an important economic or financial interest of the State or of the European Union, including monetary, budgetary and taxation matters; the protection of the data subject or the rights and freedoms of others; or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority (compare Article 27 Loi 2002), which means usually in

[10] Article 26 (1) Loi 2002.

the cases that are established as reasons for demanding access to stored data as defined by the transposing Act.

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

Compare answer to question 18.

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?

The law transposing the Directive remains silent on this issue.

According to Article 126 (1) CIC a person concerned can claim the annulment of the orders of the juge d'instruction when justifying a legitimate interest, for example in a case in which the juge d'instruction ordered the access for crimes which do not fall under the relevant category of crimes punished with a sentence of a year or over.

In case that the data are unlawfully accessed, Articles 5 (6) and 9 (6) Loi 2005 provide for criminal sanctions:

> "Any person who contravenes the provisions of paragraphs 1 to 5 of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question."

The intervention of CNPD is additionally provided for in Article 12 Loi 2005 which makes reference to the Loi 2002. According to this act, the CNPD disposes of several administrative sanctions, such as

> "(a) alert or admonish controllers who have violated the obligations imposed upon them by Articles 21 to 24; (b) block, delete or destroy data that have been subject to a processing operation contrary to the provisions of this Law or its implementing regulations; (c) impose a temporary or definitive ban on a processing operation that is contrary to the provisions of this Law or to its implementing regulations; (d) order publication of the prohibition decision in full or in extracts in newspapers or by any other method, at the cost of the person sanctioned".[11]

Articles 38 and 39 of the Loi 2002 provide that "in the event of a processing operation that violates formalities provided for under this Law being undertaken, any person is entitled to legal remedies".[12] This includes the case of a notification not being issued as provided for by law. However, in the context of access to retained data, the exceptions (when there is no obligation to inform) probably will

[11] Article 33 Loi 2002.

[12] Article 38 Loi 2002.

be applicable, e.g. the exceptions mentioned in Art. 27 (1) such as national security or combating certain crimes.

An "action for discontinuance" can be invoked before the courts by the injured party or the national data protection commission when it has declared itself responsible in respect of the claim.[13] The action is "admissible even when the illegal processing has ceased or is not likely to recur".[14]

Finally, the injured party may invoke Article 1382 Code civil (Civil code)[15] which provides for the possibility to institute a civil action.

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.

Article 5-1 of the Loi 2005 refers to Article 22 and 23 of the general security provisions entailed in the general data protection act (Loi 2002).

The Loi 2002 includes in Article 22 technical guidelines and in Article 23 the following security provisions:

> Article 23 Special security measures
> Depending on the risk of the breach of privacy, as well as the state of the art and the costs associated with their implementation, the measures referred to in Article 22, paragraph (1)
> must:
> (a) prevent any unauthorised person from accessing the facilities used for data processing (monitoring of entry to facilities)
> (b) prevent data media from being read, copied, amended or moved by any authorised persons (monitoring of media);
> (c) prevent the unauthorised introduction of any data into the information system, as well as any unauthorised knowledge, amendment or deletion of the recorded data (monitoring of memory);
> (d) prevent data processing systems from being used by unauthorised person using data transmission facilities (monitoring of usage);
> (e) guarantee that authorised persons when using an automated data processing system may access only data that are within their competence (monitoring of access);
> (f) guarantee the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (monitoring of transmission);
> (g) guarantee that the identity of the persons having had access to the information system and the data introduced into the system can be checked and recorded ex post facto at any time and by any person (monitoring of introduction);
> (h) prevent data from being read, copied, amended or deleted in an unauthorised manner when data are disclosed and data media transported (monitoring of transport);
> (i) safeguard data by creating backup copies (monitoring of availability).

---

13 Article 39 (1) Loi 2002.

14 Article 39 (2) Loi 2002.

15 Accessible at: http://www.legilux.public.lu/leg/textescoordonnes/codes/index.html.

The terms “state of the art” and “costs associated with their implementation are not specified by law or jurisprudence, as there is hardly any jurisprudence on the interpretation and application of data protection related provisions in Luxembourg.

General security provisions are also briefly dealt with in Article 3 of the Loi 2005:

> Article 3 – Security
> 1. The service provider must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the operator with respect to network security. In the event of any breach or serious risk of a breach of the security of the network or services, the service provider and, where necessary, the operator shall take appropriate remedial measures, at its/their sole expense.
> 2. Without prejudice to the foregoing, the service provider and, where necessary, the operator must inform the subscribers of any imminent risk of a breach of the security of the network or services which may compromise the confidentiality of communications, and of any possible remedies, including an indication of the likely costs involved.

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

Normally, the data has to be destroyed after the retention period expires except for data to which access was legally allowed and which were consequently preserved (Article 5-1 (2) Loi 2005). There is no specific time-limit for the storing of the accessed data.

The general handling of personal data in criminal procedures is based on Article 48-24 CIC. This provision refers to a specific regulation[16] which lists different categories of data that can be retained and accessed. This regulation does not include a time-limit for storing as it refers itself to other specific regulations for different sectors[17] which regulate the details of retention in the relevant fields. Therefore, there is no general time-limit for the storing of data in criminal files.

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.

Similar to Article 3 (1) and (2) of the Directive 2006/24, Article 1, 5 (1) (a) and Article 9 (1) (a) Loi 2005 oblige any service provider or operator in the electronic communication sector carrying out processing of personal data in the context of the

---

16 Règlement grand-ducal du 22 juillet 2008 portant exécution de l`article 48-24 du Code d`instruction criminelle et de l`article 34-1 de la loi modifiée du 31 mai 1999 sur la police et l`inspection générale de la police, Mémorial A, N° 126, p. 1909; accessible at: http://www.legilux.public.lu/leg/a/archives /2008/0126/a126.pdf#page=5.

17 For instance to the Règlement grand-ducal du 21 décembre 2004 portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière et modification du règlement grand-ducal du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales, Mémorial A, N° 209, p. 3788; accessible at : http://www.legilux.public.lu/leg/a/archives/2004/0209/a209.pdf#page=6.

supply of publicly available electronic communications services[18] over the public communication networks[19] to store the data. Further specifications or distinctions are not made.

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?

No general exemptions are specified in the acts transposing the Directive.

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?

Article 5 (1) and (2) Loi 2005 in the original version which transposed Directive 2002/58 already obliged service providers and operators in 2005 to retain their data and hold them available for 12 months for judicial authorities for the investigation, detection and prosecution of crimes without further specifying which data categories were concerned. The categories should have been regulated in a "Règlement grand-ducal" according to Article 5 (1) (a) Loi 2005 in the original version. This however did not happen before entry into force of the transposing Act in 2010.

The data could be further requested by the "competent authorities" for using them in law suits, in particular in interconnection or billing disputes (Article 5 (2) Loi 2005.

The retention period of 12 months was reduced to 6 months by an amendment of the general data protection act in 2007 (Loi 2002), see above question 13.

---

[18] According to Article 2 (k) Loi 2005, "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. The supplier of electronic communications services is hereinafter referred to as the "service provider". This definition mainly corresponds to the definition in Article 2 (c) Directive 2002/21/EC on a common regulators framework for electronic communications networks and services, OJ 2002, L-108/33.

[19] According to Article 2 (i) Loi 2005, "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. This definition mainly corresponds to the definition in Article 2 (a) Directive 2002/21/EC on a common regulators framework for electronic communications networks and services, OJ 2002, L-108/33.

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)?

No, there are no further obligations.

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)?

No figures 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?

No, the parties do not receive any form of reimbursement.

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

So far, no rules are in place.

According to Article 5 (1) (a) and Article 9 (1) (a) Loi 2005, such rules can be determined in a Règlement grand-ducal but so far, no regulation governing this issue was adopted. The preparatory documents of the Parliament state that this regulation was considered as being not necessary so far because the providers transmit the data in an "intelligible" form to the juge d'instruction. In other words no problems have occurred so far that would give reason to adapt the statutory situation.

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.

Articles 5 (6) (retention of traffic data) and 9 (6) (retention of location data) of the Loi 2005 provide for:

> "any person who contravenes the provisions of paragraphs 1 to 5 of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 Euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question."

According to Article 25 of the Loi 2002:

"Any party who carries out a processing operation in breach of the confidentiality and security rules referred to in Articles 21, 22 and 23, will be liable to a prison sentence of between eight days and six months and a fine of between 251 and 125,000 Euros or just one of these penalties. The court hearing the case may order the discontinuance of processing that is contrary to the provisions of Article 21, 22 and 23, subject to a financial penalty the maximum amount of which will be set by the said court."

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?

The decisions of the juge d'instruction or of the president of the judges' chambers of the appeals court are communicated directly to the operators (Articles 67-1 and 88-2 CIC). The juge d'instruction can delegate the investigative measures to the police according to Article 52-1CIC.

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?

No.

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?

So far, no general rules have been adopted in the course of the Directive's transposition regulating the exchange of data between the different bodies.

According to Articles 67-1 and 88-1 to 88-4 CIC, only the judicial authorities (juge d'instruction, the president of the judges' chambers of the appeals court or the prime minister) can access the data.

Not specifically in the context of communications data there is a chapter in the CIC that governs the exchange of personal data between public entities and the public prosecutor (chapter IX CIC). This does not however directly apply to the situation concerned here. It is imaginable that authorities might apply those rules but it is unclear whether a court would uphold such an application in this context. Therefore there is no direct exchange possible or foreseen between the different branches and it remains unclear whether it is at all possible.

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)?

The exchange with third countries is not expressly forbidden. There are no special provisions governing the exchange of the data retained. Therefore, this follows the usual procedure of letters rogatory.

Article 8 (1) Loi 2002 (general data protection act) refers to the processing of data for the purpose of criminal investigations (judicial data) and legal proceedings which will be performed pursuant to the provisions of the CIC, the Civil Procedure Code[20], the Act relating to Procedural Rules before Administrative Courts[21] or other laws (Article 6 (2) (i) in connection with Article 8 (1) of the Loi 2002.

There is a general chapter on the transfer of data to third countries (Art. 18 et seq. Loi 2002). For data exchange at EU level and only concerning criminal matters, the act transposing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is applicable (Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale amended by the loi du 27 October 2010[22]). The exchange with third states depends on the international agreements in force. Luxembourg is party to the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe and its Additional Protocol regarding supervisory authorities and transborder data flows (No. 181), but not to the Cybercrime Convention No. 185 (Luxembourg signed on 28 January 2003, but has not yet ratified this Convention).

---

20 Nouveau Code de procédure civile (3 août 1998), Mémorial A, no. 64 from 17 August 1998, last modified by Loi du 5 juin 2009, Mémorial A, no. 134 from 15 June 2009, p. 1889, accessible at: http://www.legilux.public.lu/leg/textescoordonnes/codes/index.html.

21 Loi du 21 juin 1999 portant réglement de proc.dure devant les juridictions administratives, Mémorial A, no. 98 from 26 July 1999 last modified by Loi du 28 July 2000, Mémorial A no. 71 from 9 August 2000; accessible at: http://www.legilux.public.lu/leg/a/archives/1999/0098/a098.pdf#page=2

22 Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale, Mémorial A – No. 98 from 18 September 2000 amended by the loi du 27 October 2010 Mémorial A – No. 194 from 3 November 2010.

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)?

The CNPD is responsible for overseeing compliance with the security rules entailed in Article 22 and 23 of the Loi 2002 and may take administrative disciplinary sanctions (Article 32 and 33 Loi 2002) in case of non-compliance.

The CNPD is an independent body exercising a legal as well as a technical control. It is not directly controlled by any ministry or other public body (cf. esp. Art. 35 (8) Loi 2002). A sort of "tutelage" of the ministry of the state is however exercised inasmuch as the financing of the CNPD comes from the ministry's budget. However, in practice the CNPD has a high level of independence.

The use of the data in criminal procedure (the "judicial data") underlies the ordinary supervision of the work of the juge d'instruction within the so-called "cabinets d'instruction". The juge d'instruction has an independent and impartial standing and does not underlie directly the supervision of the "Parquet Général". The latter may request the juge d'instruction to collaborate in specific cases.

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?

No.

If so, please answer to the following questions:

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

/

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

/

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?

/

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)?

No.

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?

The data are to be stored locally by and at the premises of the service providers.

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?

The outsourcing or the transfer to third countries is not explicitly forbidden in the law transposing the Directive and might therefore take place according to the general rules applicable to third states of the Loi 2002.

According to Article 18 of the Loi 2002, transfer is possible to countries providing an adequate level of protection whereby the level of protection afforded by a third country must be assessed by the controller (Article 18 (2) Loi 2002). Derogations from the adequacy requirement are entailed in Article 19 Loi 2002 and allow for transfer if:

> (1) (a) the data subject has given his consent to the proposed transfer; or
> (b) the transfer is necessary for the performance of a contract to which the data subject and the controller are parties or the implementation of pre-contractual measures taken at the data subject's request; or
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of a legal claim; or
> (e) the transfer is necessary in order to protect the vital interests of the data subject; or
> (f) the transfer occurs from a public register as provided in "Article 12, paragraph (2) letter (b)."
> (2) In the case of a transfer made to a third country that does not offer an adequate level of protection within the meaning of Article 18, paragraph (2), the controller must, at the request of the Commission Nationale, provide the Commission within fifteen days with a report stating the conditions under which it made the transfer."

(3) Without prejudice to the provisions of paragraph (1), the Commission Nationale may authorise, as a result of a duly reasoned request, a transfer or set of transfers of data to a third country that does not provide an adequate level of protection within the meaning of Article 18, paragraph (2) if the controller offers sufficient guarantees in respect of the protection of the privacy, freedoms and fundamental rights of the data subjects, as well as the exercise of the corresponding rights. These guarantees may result from appropriate contractual clauses. The controller is required to comply with the decision of the Commission Nationale.
(4) Any party who transfers data to a third country in violation of the provisions of this Article will be liable to a prison sentence of between eight days and one year and a fine of between 251 and 125,000 euros or just one of these penalties. The court hearing the case may order the discontinuance of a transfer that is contrary to the provisions of this Article, subject to a financial penalty the maximum amount of which will be set by the said court.

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

a) no data are retained beyond what is permitted?

There are no specific measures implemented that are made public. There is supervision of the work by the CNPD (e.g. by on-site-visits) but beyond that it is not possible to identify such measures. This answer in principle applies to all following subquestions.

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)?

Judging from information on this question that was available in Luxembourg by the competent bodies, there are no technical interfaces existent that enable the state to access directly the data retained. The original plan of creating a central storage system with such access was given up so there is no direct access today.

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

cf. above; the level of protection of the data is the same as any file in criminal procedure due to the quality as "judicial data" described above.

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.

At the provider's level, apart from the measures mentioned in question 21, some operators have implemented the following measures (although they are not obliged to do so):

- data separation (traffic data used for business purposes are separately stored from data used for law enforcement purposes)

- written IT policy

- training of the relevant staff, whereby every operator has his own methods (e.g. monthly meetings, training once a year and on the spot, collaborative elaboration of procedures, electronic news and regular meetings, intranet, email; training of team leaders by department managers etc.)

- password identification, authorisation procedures and a very limited number of staff with access rights

- physical protection in form of personal access cards without which access is not possible

- In addition the work of the Institut Luxembourgeois de Régulation (ILR) needs to be mentioned because in a regulation[23] it has set the technical details to be respected by the network providers in case of communication interception.The ILR is the supervisory body for the electronic communications networks and services. (legal package "paquet télécom" of 2005)[24]. These safety issues are also applicable in a comparable manner to data retention.

- Finally, Article 41 (1) of the Loi 2002 refers to a regulation which sets the technical details of the access by judicial authorities to inventory data of electronic communication services.[25] These standards, even if not directly applicable, set a framework of reference for the judicial access to traffic and location data.

---

23 Règlement 08/134/ILR, Mémorial A, no. 188 from 1 December 2008 with an Annex.

24 http://www.legilux.public.lu/leg/a/archives/2005/0073/a073.pdf#page=20); for further details see: http://www.ilr.public.lu/communications_electroniques/index.html

25 Règlement grand-ducal , Mémorial A, no. 209 from 30 December 2004.

- At the level of the authorities accessing the data:

- Article 458 CP obliges officials to professional secrecy.

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

cf. above

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)?

No specific information, cf. above

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

No specific information, cf. above

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)?

Depending on the operator, different possibilities exist:

- the operator can carry out an audit covering financial aspects, which generally includes some checks on the security. This however cannot be considered as a security auditing particularly dedicated to traffic data.

- independent "infiltration" tests

- external control by the CNPD

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?

The technical requirements for interception of communication that were laid down in Règlement 08/134/ILR (see question 40 d)) and the Annex apply mutatis mutandis.

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.

Apart from the procedures provided for in Articles 67-1 and 88-1 to 88-4 CIC (the decisions to access the data of the juge d'instruction or of the president of the judges' chambers of the appeal court are communicated to the operators), there is no

other existing procedure. In reality this means that providers follow up the request by providing the data to the requiring body. This has to happen in a speedily manner ("dans les meillieurs délais").

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?

The act transposing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is applicable for cross-border requests (Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale amended by the loi du 27 October 2010[26]). There is no specific information about the working language, so it is regularly the usual working languages French and German.

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).

So far, a public or an academic debate on data retention has not yet taken place. The CNPD confirmed that it has not received a single official question relating to data retention from the citizens so far. Journals did briefly discuss the German Constitutional Court judgment on the German data retention law in March 2010, but the articles did not consider the topic as being a problem in Luxembourg.

The CNPD however issued an opinion on data retention before the "Loi 2005" came into force.[27] The opinion also refers to the German Constitution Court judgment on data retention in March 2010 and proposed minor changes to the "Loi 2005". Almost all of them were considered in the finally adopted amending law to "Loi 2005". One exception concerns the offences which give reason to the judiciary to access to the data of service providers. The CNPD argued in favour of a limited list of offences triggering such an access right (and listing these enumeratively). The

---

[26] Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale, Mémorial A – No. 98 from 18 September 2000 amended by the loi du 27 October 2010 Mémorial A – No. 194 from 3 November 2010.

[27] The opinion available at: http://www.cnpd.public.lu/fr/decisions-avis/2010/04/retention-donnes/avis_CNPD_projet_loi_6113.pdf.

adopted "Loi 2005" however provides for the above mentioned one year threshold which in effect entails more potential application cases.

In addition, the CCDH[28] issued one opinion on the amendment of the Loi 2005 in 2010. Like the CNPD, the CCDH also argues in favour of a limited list of offences and strongly opposes the one year threshold which was determined by the amendment of the Loi 2005 in 2010. The CCDH proposes to limit the offences triggering an access right to offences related to terrorism, organised crime and the "fight against drug related crime". Moreover, the CCDH criticises that the security rules applicable to the providers are not specifically enumerated in the Loi 2005.

Summarising, the CCDH proposed the following recommendations:

- the scope[29] of the access to the data should be clearly defined
    - the questions of security should be strictly regulated in the Loi 2005
- the list of the offences triggering an access right should be limited
- only judicial authorities should have the right to order access to the data
    - the possibility to delegate the storage of the data to another body than at the service provider should be precisely formulated (this possibility (e.g. like in the Netherlands) was removed in the final version of the Loi 2005; this however does not exclude that it is still possible, see above)
    - effective, proportional and dissuasive sanctions should be in place in case of violations of the law

All in all, either the society seems not to be aware of the retention (possibly due to the fact that there is not much information disseminated via the media and no additional information is publicly available beyond the preparatory materials of the Law and the debates in Parliament as well as the positions of CNPD and CCDH) or the citizens are not convinced of a necessity to discuss data retention in depth. This can also be seen that hardly any specific articles have been published in either the legal databases or newspapers, one exception being a descriptive piece concerning the new law in a newspaper of September 2010.

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)?

No.

---

28 Commission consultative des droits de l´homme du Grand-Duché de Luxembourg. The opinion is available at: http://www.ccdh.public.lu/fr/avis/2010/avis_CCDH_PL_6113.doc.

29 In the opinion of the CCDH this word is only used once and presumably concerns the list of offences that allow access and in that sense overlaps with the third argument mentioned which focuses more on the fact that it should be a complete enumeration and at the same time limited list.

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 no statistics so far, but Article 1 (6) Loi 2005 provides that the national data protection commission annually transfers statistics to the European Commission about the retention of the data. For this purpose, the service providers and operators have to provide the CNPD with information relating to:

- the cases in which the data were transferred to the competent authorities in accordance with the applicable legislation
- the time between the date of retention and the date of transmission to the competent authorities
- the cases in which the requests could not be satisfied

Such statistics do not contain personal data.

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?

No.

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?

No.

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) law30 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

Article 11 (3) of the Luxembourgish Constitution protects the right to private life, Article 28 protects the secrecy of letters, including communication.

Freedom of expression and information/freedom of the media, protected by Article 24 of the Luxembourgish Constitution, freedom of thought, religion/belief and/or conscience (Article 19 of the Luxembourgish Constitution) and basic rights concerning the judiciary (Articles 12, 13 and 14 of the Luxembourgish Constitution) can potentially be affected by data retention.

The fundamental rights mentioned result from the constitution and in part only from other legal acts or from case-law. There is one important law protecting the right to private life in a very general manner that sets basic rules but is not applicable in a specific manner for data retention.[31]

The scope of the protection of fundamental rights depends on the relevant case law. However, there is only little jurisprudence on constitutional and fundamental rights issues in Luxembourg. Actually, one of the main points of criticism relating to the Luxembourgish Constitution is that the scope of application of the different fundamental rights are formulated in an imprecise manner. Inter alia because of this, currently a constitutional reform is underway and an amendment is foreseen in 2011.

The current wording of Article 28 only protects the secrecy of letters, but the article is interpreted as if it would protect the secrecy of telecommunication. The draft bill to reform the constitution will also contain an article including the protection of communication in general.

Constitutional law remains silent on this issue.

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?

Article 11 (3) of the Constitution (protection of the right to private life) refers to exemptions provided by law and Article 28 of the Constitution does not explicitly refer to limitations.

---

30 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).

31 Loi du 11 août 1982 concernant la protection de la vie privée, Mémorial A-86, p. 1840, from 12 october 1982.

There are no specific limitations included in Luxembourgish constitutional law as regards the content of a law which restricts fundamental rights. The jurisprudence nonetheless applies the rule of law and regularly makes reference to Belgian case law which interprets the rule of law. The commission working on the reform of the Luxembourgish Constitution proposed to add to the current Article 51 of the Constitution one paragraph which would specify that Luxembourg is constituted as an "Etat de droit" (state under the rule of law).[32]

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?

/

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?

As there is no interpretation available on this question and the amount of jurisprudence is generally limited in constitutional issues, it is not possible to derive such limits or balancing rules, not in general nor in the individual case.

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)?

No.

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?

There is no in-depth discussion in academia so far on these aspects. From our perspective the restrictions are in line with the (insofar limited) protection granted by the constitution. The limits are not clearly defined.

---

[32] Compare Ergec, Rusen, Deux concepts constitutionnels nouveaux: l`Etat de droit et la dignité humaine, Journal des Tribunaux Luxembourg 2009, pp. 180-184.

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)?

Data are retained in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of criminal offences, which entail a maximum sentence of at least one year according to article 5 (1) (a) and Article 9 (1) (a) Loi 2005.

It is not evident whether there is a general obligation in national law for private actors (businesses, citizens) to assist law enforcement agencies in their tasks, e.g. by providing evidence that might be used to investigate, prosecute or detect a criminal offence. This would have to be analyzed by an expert in Luxembourgish criminal procedure law as well as the law governing police investigations.

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

No.

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?

In Luxembourg, international treaties have to be transposed into national law via the the ordinary legislative procedure. The laws created on this basis do not have any specific priority since there is no such hierarchy of norms; instead, they have the status of an normal Luxembourgish act (Article 37 Luxembourgish Constitution). They do have a special validity though, since (Article 95ter Luxembourgish Constitution) a review of constitutionality is excluded for these laws.

However, international treaties are in general, both in jurisprudence and academic viewpoints, widely accepted as having a specific character that gives them direct effect – if they contain subjective rights – and applicability in national law beyond the transposition act. This particular position of international treaties and the transposing acts has been expressly stated on several occasions by courts and observers concerning the ECHR.[33] Beyond that, judges can in their decisions set aside – not: annul – national law if they see a violation of an international law treaty in a specific provision.

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

[33] Compare for instance: Conseil d'Etat, 21 mars 1990, n° 8300; Tribunal d'arrondissement de Luxembourg, 31 mars 1993, Bulletin des droits, de l'homme, n° 1, 1993, p. 107, obs. Luc Weitzel.

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?

In general, Directives have to be transposed into national law via the ordinary legislative parliamentary procedure described below. Usually the provisions of a Directive are copied word for word in this process. However, European law, including Directives, plays an important role and even if a Directive is not yet transposed, national judges will nevertheless apply its provisions as if it was already in force. There is no evident limitation of the use of this "rule" by national judges.

During the normal legislative procedure, which is initiated by a governmental (projet de loi) or parliamentary step (proposition) and then discussed in Parliament (Chambre des députés), the Conseil d'Etat examines the proposals and comments on on their constitutionality, legality and usefulness. The opinion by the Conseil is basis for the debate and possible amendments by the Parliament. A first vote is followed by a second vote within three months, but the Parliament can and regularly does ask for a dispensation of that second vote which the Conseil d'Etat has to agree to. After a majority has decided on the law, this has to be signed by the Grand-Duc and the ministers which are responsible in the specific field. Three days after having been published in the Mémorial (Official Journal) the law enters into force if no specific provision on this is contained in the law.

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?**

Without going into a deeper analysis of this very fundamental question on first observation there is no limitation vis-à-vis the EU. Indeed, there is no case law at all on the relation between European law and the national constitution and especially not in the sense of a controversy comparable to "Solange, Maastricht, Bananenmarkt-VO, Lissabon" of the BVerfG.

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 framework for data retention was set by Loi 2005 and Règlement 2010. In the preparation of this the so-called "Service des médias et des communications" (SMC) was involved. This "service unit" is a part of the governmental administration working for the minister responsible for the media (currently the Minister for Communications and the Media). As such, it is staffed with state employees that provide assistance to the minister, but also for the other institutions created by the law in the field of the media. However, in the legal framework set by the Parliament the roles concerning data retention are solely distributed between the CNPD (supervision of the providers) and the judicial department (Parquet Général) in

charge of the juge d'instruction. There is no further involvement by the Ministry. The ILR is involved indirectly by setting technical standards to be applied by the operators.

There are no regional territorial entities that are vested with own powers.

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

No.

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?

The advisory opinions of CNPD and CCDH have given some indications of possible further improvements. From our point of view there would be possibilities for clarification of legal requirements, although it is well possible that this will happen in the application and interpretation of the law by the courts. Also, some rather political issues (awareness) could play a role.

- specifying the list with the accessing authorities that can demand access to the data (transparency)

- describing the access procedure of the judicial authorities in detail (in an executive regulation or by making the information public)

- enacting concrete technical security measures to protect the data retained (applicable to all the service providers) beyond the Règlement of the ILR; alternatively proposing self-regulatory provisions to be prepared and imposed by the providers themselves

- Raising awareness / launching a public debate on the need and limitations of data retention

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

Luxembourg

*Prof. Dr. Mark D. Cole / Dr. Franziska Boehm**

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*?

Currently, there is no Luxembourgish provision providing for a right to communicate anonymously, neither in the constitution nor in other legislation. Since there is only little jurisprudence concerning the interpretation of the constitution and no case relating to this issue, there is no discussion of whether the right can be derived from existing provisions either. In addition it needs to be pointed out that there is no general prohibition of anonymous communication either.

Related to the question of anonymity, the rules concerning secrecy of communication are as follows: The Luxembourgish constitution provides for a right of secrecy of letter guaranteed by article 28[1], which also extends the protection to be created by the law to telegrams which dates back to the introduction of the provision. This article is currently under review, too, in the framework of the overall revision of the constitution. If the proposed amendments are adopted, the applicability of the norm would be extended to every kind of private communication.

2. Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country (or have already been adopted after your replies to the first questionnaire, e.g. by "Loi du 27 février 2011 sur les réseaux et les services de communications électroniques"). How strong (in terms of support they get by the public) are the different arguments uttered in

---

* The author *Cole* is Associate Professor for the Law of the New Information Technologies, Media and Communications law at the University of Luxembourg (www.medialaw.lu), the author *Boehm* is research associate at the University's Interdisciplinary Centre for Security, Reliability and Trust (SnT).

1 http://www.legilux.public.lu/leg/textescoordonnes/recueils/Constitution/Page_de_garde.pdf.

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?

The "loi du 27 février 2011 sur les réseaux et les services de communications électroniques"[2] transposes Directives 2009/140 and 2009/136 in national law. This act however does not include the data protection issues from the revision of the Directive. From the start, it was planned to regulate these aspects in a separate piece of legislation.[3] Meanwhile, a revised version of the Loi 2005 has been drafted and passed and entered into force on September 1st 2011.[4] It mainly involves new security and information provisions and confidentiality rules.

In particular, its art. 3 entails an enhanced protection of individuals. As regards the security measures described in question 21 of the first questionnaire, the revised version of the Loi 2005 adds provisions protecting the data retained against unauthorised access in the way that the service providers must guarantee that only authorised persons are entitled to have access to personal data. Moreover, service providers are obliged to protect personal data against accidental destruction, loss, alteration and dissemination. They must further assure that there are security measures in force with regard to the use of the personal data. The CNPD is responsible for the supervision of these measures.

Further, art. 3 para. 3 of the revised version of the Loi 2005 provides an information right for persons concerned. In case of the violation of data protection rights, the service providers have to inform the CNPD immediately. If the violation negatively affects personal data or private life of a subscriber or a private person, the service provider must also inform the person concerned. This notification duty does not apply, if the service providers prove, to the satisfaction of the CNPD, that they have applied the necessary security measures and that the latter have been applied to the data concerned. As foreseen also in the Directive, such security measures concern a technological protection that renders the data unintelligible to any person who is not authorised to access it. The CNPD has also the right, after having examined the violation, to force the service provider to inform the person concerned.

---

2 Loi du 27 février sur les réseaux et les services de communications électroniques, Mémorial A no. 43 of 8 March 2011, accessible at : http://www.legilux.public.lu/leg/a/archives/2011/0043/a043.pdf#page=2.

3 Compare the summary of the act (last sentence): http://www.chd.lu/wps/portal/public/RoleEtendu?action=doDocpaDetails&id=6149#.

4 Compare Loi du 28 juillet 2011 portant modification 1) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électronique; 2) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l`égard du traitement des données à caractère personnel; 3) de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l`Etat; 4) du Code de la Consommation, Mémorial A-N° 172, p. 2938 of 10 August 2011; accessible at: http://www.legilux.public.lu/leg/a/archives/2011/0172/2011A2938A.html?highlight=.

As regards proposals for improvements, there is no intensive public debate on the need and limitations of data retention in Luxembourg. Only a very limited amount of press articles questioning the need of data retention or discussing its impact have been published so far.[5] The political debate regarding the introduction of data retention was also rather limited and oriented towards practical requirements on how to introduce the EU obligation rather than critically questioning it in view of fundamental rights. Currently, there are no discussions about a "quick-freeze" option as an alternative to the new framework. Please refer also to our answer in relation to question no. 45 of the first questionnaire.

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?**

   There is no single source specifying a general duty for private actors to cooperate with public authorities for the detection, investigation and prosecution of criminal offences or other purposes in Luxembourg.

   However, several specific situations can lead to such a duty, for various reasons.

   It can be directly the case when private persons are deemed to carry out a public service, or when they are required by public authority to support public authorities in certain circumstances:

   (i) in case public authorities decide to use a formal requisition which will oblige people to collaborate, for example when a witness is required during a trial.[6]

   (ii) in the case of war any private person.[7]

   (iii) when a due diligence is expected for specific criminal offences as is the case in the framework of the fight against money laundering, where private professionals are required to detect and perform prior checks, as well as communicate to public authorities any suspicion they have regarding their clients.[8]

---

5 Compare e.g. "Vorratsdatenspeicherung wirft Fragen auf", Luxemburger Wort of 6 April 2011, pp. 2-3.

6 Compare article 77 CIC.

7 Compare article 4 Loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, Mémorial A, n° 98 of 24.12.1981, accessible at: http://www.legilux.public.lu/leg/a/archives/1981/0098/a098.pdf#page=2.

8 Compare articles 2, 4 and 5 Loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme portant transposition de la directive 2001/97/CE du Parlement européen et du Conseil du 4 décembre 2001 modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, Mémorial A n° 183 of 19.11.2004, accessible at: http://www.legilux.public.lu/leg/a/archives/2004/0183/a183.pdf#page=2.

It can be indirectly the case in situations where criminal offences involve a dangerous situation for an individual. Under such circumstances there is a general rule according to which witnesses are obliged to actively help directly or at least – if there is otherwise a real danger for themselves – to immediately contact specialised services: in this context, the witness cooperates directly or is at least obliged to inform public authorities.[9]

In addition to the situations mentioned above, according to the revised version of the Loi 2005, mobile phone or fix-line service providers offering access to the harmonised European emergency number 112 as well as other emergency numbers determined by the regulatory authority have to immediately and without individual request transfer the data concerning those calls (telephone number, name, address, location data etc.) to the responsible authorities.[10]

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?**

In the CIC there is no text specifically stating that there is a right to refuse to deliver evidence against oneself. However, this right is enshrined in article 6 of the European Convention on Human right as applied by the Strasbourg Court in its respective case law (compare Saunders vs. United Kingdom of 17 December 1996, or Funke vs. France of 25 February 1993). Luxembourg is a Member State of the Council of Europe and Luxembourgish judges generally comply with the respective obligations as interpreted by the jurisprudence of the European Court of Human Rights when they fulfil their mission. As a result, in case that this specific aspect of the "right to a fair trial" is questioned in front of a Luxembourgish Court, judges analyse it in the light of the Strasbourg Court's jurisprudence, and therefore recognize a "right to refuse to deliver evidence against oneself".[11]

In addition, the right to refuse to testify/to deliver evidence against oneself is indirectly recognised in Luxembourg by article 73 CIC which prohibits that the juge d'instruction, the prosecutor or police officers to interrogate persons as witnesses if "serious indications" for their culpability in that case exist.[12] Moreover, article 72

---

9 Compare article 410-1 and 410-2 CP.

10 New art. 7 of the revised Loi 2005.

11 Compare a case specifically regarding this topic: Judgement of the "Tribunal d`arrondissement" (regional court) no. 2362/2000 of 30 November 2000.

12 Article 73 CIC : "Le juge d'instruction chargé d'une information, ainsi que les magistrats et officiers de police judiciaire agissant sur commission rogatoire, ne peuvent, dans le dessein de faire échec

CIC entails the right of the suspect to refuse to testify as a witness if the potential victim has enacted civil proceedings and acts as a (civil) plaintiff against the suspect.

Also, special provisions with regard to lawyers or journalists exist. The lawyers profit from the professional secrecy (art. 35 loi sur la profession d`avocats[13]) which in principle can include to refuse to deliver evidence against oneself beyond the right to refuse to testify against a client, although it is not directly formulated in this way. The communication between the lawyer and his client is also protected by art. 35 (3) loi sur la profession d`avocats.Journalists profit from the right to protect their sources.[14]

In a case concerning data retained, it is difficult to establish from the provisions to what extent one of the specified rights would apply and – if so – whether and how it would conflict with data retention. In principle any information that can have negative effects need not be disclosed by a suspect (and in that way also e.g. telecommunications data), but the question would not pose itself in the case of the provider of that person's telecommunications services. If the question hints at whether an analogy could be used to exclude the use of the data because it indirectly can circumvent the protection of the suspect against disclosing his personal information, the assumption is that this would not work in a way to bar the retention and use of relevant data.

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?

The competent bodies usually store the data in the respective files, e.g. in criminal procedures in the files held by the prosecutor. As there is no electronic file system in place at the courts that would replace the paper files, this typically happens in form of CD-ROMs or paper print outs of the data that are put into the file. This files obviously are within the scope of the usual rules protecting the files, but specific security requirements are not foreseen.

---

aux droits de la défense, entendre comme témoins des personnes contre lesquelles il existe des indices graves et concordants de culpabilité."

13 Loi du 10 aout 1991 sur la profession d`avocats, Mémorial A, N° 58 of 1991, p. 1110, accesssible at: http://www.legilux.public.lu/leg/a/archives/1991/0058/a058.pdf.

14 Art. 7 of the Loi sur la liberté d`expression dans les médias, Mémorial A, N° 69 of 30 April 2010, p. 1325.

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.**

   No, there are no statistics available. The data access requests carried out by the judges are included in the files related to the respective cases so this would require an individual screening of the existing files. Depending on the case and e.g. the length during which the suspected crime occurred, the amount of the data as well as the type of the requested data can vary significantly.

B. Country-specific questions

7. **Please give your own opinion on the constitutionality of the data retention regime in your country as a whole. Has the amendment to the Constitution, envisaged for 2011, already been adopted? If so: does this bring about any fundamental changes to the constitutionality assessment?**

   The amendment has not yet been adopted. The current wording of Article 28 of the Luxemburgish Constitution only protects the secrecy of letters, but the article needs to be interpreted in a way as if it would protect also the secrecy of telecommunication. The draft bill to reform the constitution according to the current status of debate will consequently contain an article including the protection of communication in general. That supports the view of understanding the current provision broadly because the more limited wording is only a result of the technological situation at the times of its creation.

   As of now – and this would not be influenced by the proposed amendment – there is no evident breach of constitutional standards by the data retention provisions. The protection of privacy according to the Luxembourgish constitution is not extraordinarily extensive, so the retention of data for the use in specific cases by itself does not seem to be in violation or potential conflict with it. However, the situation could be different if one would regard the data retention provisions (i.e. the Directive and its national transposition) as a violation of the right to private life in Article 8 of the ECHR. Since Luxembourgish courts can directly apply the ECHR standards theoretically a negative assessment of the Luxembourgish law could be based on the assumption of a violation of the standards in the Convention. This would still not be a violation of the constitution but the effect of the fundamental rights protection via the Convention has an equal standing. Nonetheless, it is very unlikely that under the given situation a Court in Luxembourg would come to this conclusion and it is more likely that one day a citizen of one of the affected states will take a data retention case to Strasbourg.

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?

The Directive 2006/24/EC defines in art. 2 para.2 and art. 5 the kind of data to be retained. Under the condition that providers and the Member States ensure that the retained data "relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated" (and thereby the providers are complying with the law), the "secrecy of the letters", as stated in art. 28 of the Luxembourgish constitution is not be affected as such.

A draft for a complete revision of the Constitution is currently discussed within the parliament and according to that draft the secrecy of correspondence stated in art. 28 would be reformulated extending then explicitly to every type of private correspondence, irrespective of its form. This secrecy, however, is – although no explicit case law exists – obviously directed at the actual content of the communication as it was introduced to ensure the secrecy of letters, i.e. the "inside" of the letter, not the sender/recipient information. This logic applied to the modern technology would make it unlikely that the "sending information" itself (even after reform) is data protected by the secrecy provision.

9. Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.

As already pointed out in our answers to the first questionnaire (cf. esp. question 50) the problem is that it is difficult to establish general rules on such basic principles, especially if taken in view of the jurisprudence of the Constitutional Court due to the very limited amount of cases. In principle, the Court – which since its creation in 1997 has only handed down a little more than 60 cases – limits itself to very short reasoning in its decisions. In that reasoning the matter of proportionality is usually not dealt with at any length, let alone by a clear division of the different elements. The difficulty in arriving at generally applicable conclusions is intensified by the fact that the Court strictly limits the analysis to the validity of a provision in the law relevant in a specific open case at another court and thereby avoids having to go beyond the minimum arguments of why a provision can be upheld in view of that specific case. Although there are some instances in which the Court has given clearer indications about when a measure is proportionate – concerning the provision of expropriation where already the Constitution gives the standards and in the case of equality –, it has avoided to transfer these to other fundamental rights situations.[15] In the cases where a proportionality test has been used, at least implicitly a similar approach to the usual three-step-test as also inspired by the

---

15 Compare Gerkrath (ed.), La jurisprudence de la Cour constitutionnelle du Luxembourg 1997 – 2007 – Pasicrisie 2008 – in that collection specifically Cole, p. 59, 68 and also Gerkrath, p. 3, 6, 13 , Ravarani, p. 21, 29 ; Kinsch, p. 85, 97.

European Court of Human Rights analysis of the Convention rights can be observed, i.e. the legitimate aim of a measure, its rationality (i.e. being appropriate and adequate) and proportionality in view of the aim.

10. Please describe the following safeguards of the rule of law in detail:

- **requirement of a court order prior to the data request: please describe the steps the entitled body has to take in order to obtain a court order prior to the data request. What will the court examine before taking a decision on whether or not to issue the order? Are there any situations (e.g. "emergency cases") that are exempt from the requirement of a court order? If so: who will decide in these situations whether or not access to the data may be requested? Is it necessary to have a court decide on the lawfulness of the access after the emergency situation is over?**

  According to Article 5 (1) (a) and Article 9 (1) (a) Loi 2005, only "autorités judiciaire" (judicial authorities) are entitled to access. Article 5 (2) Loi 2005 refers to the judicial authorities mentioned in Article 67-1 and 88-1 to 88-4 CIC. These provisions deal with confiscation (art. 67-1) and surveillance measures (art. 88-1 to 88-4 CIC) and in doing so refer to the responsible authorities.[16]

  There are two different ways of access:

  1. In the framework of article 67-1 CIC (provisions deal with confiscation) the data request is restricted to crimes that can be punished with a maximum sentence of one year.

  The "juge d'instruction" must assess the circumstances making the measure necessary to discover the "truth", prior to the data request on his own initiative or with the technical support of the telecommunication provider.

  Then the juge d`instruction is obliged to send a report to the state prosecutor describing the circumstances of the facts which justify the requested measure and stating a time-limit (which cannot exceed a month) with regard to the measure. The time-limit is renewable.

  2. In the framework of article 88-1 to 88-4 CIC (special measures of surveillance), the procedure is exceptional and does not require a court order. Article 88-1 to 88-4 CIC, however, refer to offences of a particular gravity (88-1 lit. a) CIC). In result, the access is restricted to crimes that can be punished with a maximum sentence of two years or where a person can be considered as suspect according to determined facts or where ordinary investigation means are unsufficient because of the specific nature and circumstances of the facts.

---

[16] Articles 67-1 and 88-1 CIC mention the "juge d'instruction". In addition to acting himself he can also delegate the investigative action to the police according to Article 52-1 CIC; article 88-2 CIC refers to the juge d'instruction as well as to the president of the judges' chambers of the court of appeals.; articles 88-3 to 88-4 CIC additionally mention the Prime Minister who can also demand access to the data retained for the use of the secret service.

Prior to the data request, the juge d`instruction must justify his decision according to the specific facts of the case. The measure has to be stopped when it is no longer considered as necessary. It will automatically be stopped one month after the decision ordering the access. However, access can be renewed each time for one month, for a maximum period of one year, when a (justified) decision issued by the juge d`instruction is approved by the President of the Court of appeal, after having heard the state prosecutor.

In this case, the prosecutor can oppose the orders of the juge d`instruction within a time-limit of two days after the order was issued. The president of the judges' chambers of the court of appeals has then to decide on the relevant issue (art. 88-1 CIC).

- **rights of the data subject: please clarify under which conditions there is an obligation to inform the aggrieved party that data retained about their communications have been accessed. Is there an additional right of the aggrieved party (e.g. according to national data protection law) to get information about which data have been accessed.**

  Please refer to our answer given in questions 17 and 18 of the first questionnaire.

  The obligation to inform exists in the case of art. 67-1 CIC. Possible derogations from the 12 month time limit to notify after date of access in Article 67-1 (3) CIC are: the access order refers to a case involving a criminal association or organisation, it is related to terrorism or concerns the sale of medical substances or the fight against "toxicomanie" ("War against drugs").

  There is also a general obligation to inform about the retention of data: The Loi 2002 provides for a notification duty "when the data are collected directly from the data subject, the controller must supply the data subject, no later than the point at which the data are collected …".[17] However, this information duty shall not apply when the processing is, among others, necessary to safeguard national security, defence, public safety or the prevention, tracking down, recording and prosecution of criminal offences, including the combating of money laundering, the progress of other legal proceedings, an important economic or financial interest of the State or of the European Union, including monetary, budgetary and taxation matters; the protection of the data subject or the rights and freedoms of others; or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority (compare Article 27 Loi 2002), which means usually in the cases that are established as reasons for demanding access to stored data as defined by the transposing Act.

[17] Article 26 (1) Loi 2002.

An additional right of the aggrieved party to get information about which data have been accessed does not exist. The revised version of the Loi 2005[18] does not refer to an information duty in case of access either.

11. As regards your answer to question 15 of the first questionnaire: are there any news with regard to how jurisdiction applies the new mechanism, introduced to the Intellectual Property law, to grant access to data in civil procedures? Does this mechanism imply a right by the plaintiffs/defendants to access the data directly (with or without previous court order?), or may the data only be requested by the court?

Concerning the application of the mechanisms in the new law there are no information publicly available yet in cases where this has been the case. Further research into the use of the new information right in case of violations of author's rights has brought no results as to usage in front of courts to date.

The law is clear, however, on the question of the request to information: this newly introduced right (in transposition of Directive 2004/48/EC) does not give the right to direct access, instead such access has to be granted by court order. The actual information may result in the use of retained data that the telecommunications provider has to give to the plaintiff, but this can only happen on instruction by the court (Article 12 para. 1 of the law of 2009 (amending Art. 78 para. 1 of the Law on Intellectual Property). Also, the request for information can only be granted by the courts, if the measure is "justified and proportionate".

12. Please describe the content of the ILR regulation mentioned in your answer to question 40 d) of the first questionnaire (Règlement 2008/134/ILR) and any other regulation with regard to data security, applicable to data retention that has potentially been adopted thereafter.

For the changes with regard to art. 3 revised version of the Loi 2005 (general security measure), please refer to our answer given in question 2.

Concerning the ILR regulation: this regulation sets the technical details to be respected by the network providers in case of communication interception. It does not explicitly refer to data retention, but the safety issues mentioned in the regulation are also applicable in a comparable manner to data retention. They are entailed in an annex regulating the technical details in case of the interception of telecommunications in Luxembourg (lawful interception of telecommunications: application of ETSI standards in Luxembourg).19 The regulation as well as the

---

[18] Loi du 28 juillet 2011 portant modification 1) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électronique; 2) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l`égard du traitement des données à caractère personnel; 3) de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l`Etat; 4) du Code de la Consommation, Mémorial A-N° 172, p. 2938 of 10 August 2011 ; accessible at: http://www.legilux.public.lu/leg/a/archives/2011/0172/2011A2938A.html?highlight=.

[19] Accessible at: http://www.legilux.public.lu/leg/a/annexes/2008/annexe_05/1845-1860.pdf.

annex do not entail specific protection measures apart from the measures mentioned with regard to internal control mechanisms.

In particular: do these regulations provide for measures in one or more of the following areas:

Generally spoken the answer to the following questions is “no”, because the ILR regulation does not refer to specific protection measures. For the general obligations following from the Loi 2002, please refer to our answer to questions 21 and 40 (d) of the first questionnaire.

- **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**

  No

- **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**

  No

- **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**

  No

- **access logging**

  No

- **secure (irreversible) deletion after expiry**

  No

- **error correction mechanisms (e.g. hash functions, checksums)**

  No

- **secure data transmission (cryptographic security, postal delivery)**

  No

- **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**

  No

- **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**

  No

- **staff training/internal control mechanisms to ensure compliance with the law and other rules**

  According to art. 6 ILR regulation, the operator must establish a register of all activities related to interception measures. This register must include:

  - the identity of the person authorising the interception measure,

  - the services being object of the measure,

  - the exact operation carried out,

  - date and time of the operation,

  In addition, for the control of the register this must be at any time accessible for the respective judicial and public authorities (the authorities mentioned in art. 67-1, 88-1 to 88-4 CIC).

  The operators are also obliged to protect the information relating to the interception measures and the equipment used in an "adequate way". They are not allowed to disclose any information to unauthorized persons without the written consent of the judicial and public authority ordering the measure (art. 6 ILR regulation). Also, The respective judicial and public authorities must be informed in case of non-authorised access (or attempts of access) to obtain information of the interception measures or the equipment used (art. 6 ILR regulation).

- **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

  No

- **Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or to any data processing (in electronic communications)?**

  No, as mentioned before, the regulation sets the technical details to be respected by the network providers in case of communication interception. It does not explicitly refer to data retention, but the safety issues mentioned in the regulation are also applicable in a comparable manner to data retention.

13. As regards your answer to question 35 of the first questionnaire:

- **Does the CNPD also have the competence to monitor compliance of the providers with the data retention obligations, as far as these obligations do not refer to data protection/data security? If not: which bodies are responsible for this task? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?**

  Pursuant to art. 32 (1) of the Loi 2002, the CNPD is competent to monitor the entire data processing carried out in accordance with the Loi 2002. In addition to the CNPD, the Institut Luxembourgeois de Régulation (ILR) – the independent telecommunications regulator according to the EU electronic communications networks and services Directives – is responsible for the monitoring of network and electronic communication services. It issued the binding regulation which is refered to in above question 12.

- **Are there any external bodies responsible for supervising that the bodies entitled to obtain access to the data retained (police etc) act within the law? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?**

  The CNPD is in principle responsible for the control of the bodies accessing the data retained pursuant to art. 3 (1) and 32 (1) of the Loi 2002. However, as Art. 8 of the Loi 2002 gives specific rules on the treatment of "judicial data", there are specific rules applying that derive from the CIC or the other procedural laws. Also, this provision only allows the stocking of data referring to criminal convictions under the auspices of the competent public authority. The provision thereby sets specific standards for the processing without explicitly referring to the question of monitoring. In practice, the internal control mechanisms of the judicial authorities safeguard the respect for the law without cases existing – to our knowledge – in which the CNPD attempted at reviewing a specific data processing by a judicial authority. Certainly, persons affected by data processing of "judicial data" have the usual possibilities for review, e.g. after a request for data by a prosecutor a claim for this act to be declared void can be brought forward according to Art. 126 et seq. CIC. A form of regular external audit of the internal data processing mechanism at the judicial authorities does not take place.

  As mentioned, there is no explicit provision limiting the competence of CNPD although for the field of "judicial data" according to Art. 8 Loi 2002 there is reference made to the usual rules of criminal and other procedure law. At the same time, there is a differentiation made between the data use by the judicial authorities mentioned there, in short courts and prosecutors, and the use of data by the police and comparable institutions (compare art. 17 Loi 2002) for which a specific monitoring body is foreseen in para. 2. A comparable provision/specific body does not exist for the judicial data processing and – according to available information – in practice the monitoring happens internally in the competent bodies. However, the data only "transfer" into being judicial data when

requested and joined to the investigation files at the competent body so the processing of the data in advance of that is certainly within CNPD's monitoring realm.

14. **From your answer to question 23 of the first questionnaire, I understand that, as a result, only electronic communications service providers are obligated to retain data under these rules, whereas operators of public communications networks are, as such, not obligated. Is this understanding correct?**

No, Article 1, 5 (1) (a) and Article 9 (1) (a) Loi 2005 refer to any service provider or operator in the electronic communications sector carrying out processing of personal data in the context of the supply of publicly available electronic communications services over the public communication networks which also includes the network providers themselves, compare also with art. 1 of the revised version of the Loi 2005 that now explicitly also refers to public communications networks.

15. **As regards your answer to question 59 of the first questionnaire, just to clarify that I correctly understand this point: from your answer to the question, it seems to me that this rule goes far beyond the ECJ jurisprudence on the principle of direct effect (cf. case no. 26/62, Van Gend) in two aspects:**

1) for a directive to take direct effect in Luxembourg, its transposition period does not necessarily have to be expired, as it is applied from the date of its entry into force on;

2) the prerequisites set by the ECJ (i.e. that the directive is a) sufficiently clear and precise, b) unconditional and c) confers a specific right to citizens) do not have to be fulfilled. Would you subscribe to this understanding? If so: how do the national courts handle the cases of a directive the wording of which is not "sufficiently clear and precise"?

No, concerning both points. The understanding goes beyond what we meant to express in our first answer. Although indeed Luxembourgish courts very open to a direct application of a Directive this does not mean a general application in advance of the expiry of transposition deadlines nor in cases of an unclear formulation of the Directive's provision except if that would be open to a reasonably expectable result by interpretation.[20] An extensive search on the internal database concerning all cases where this question has played a role previously confirms that Luxembourgish courts accept and respect the direct application of Directives, but within the conditions set by the Court of Justice of the European Union, which the national Courts explicitly refer to. Therefore, concerning the potential application of a directive (or certain rules contained therein) even before the expiry of the deadline for transposition, unsurprisingly there are examples where this possibility was explicitly ruled out.[21]

---

[20] Cf. decision in an urgent procedure, Trib. d'arrond. Lux., of 25 April 2001,LJUS Doc. No. 99820795.

[21] Cf. judgment of the Cour d'Appel rendered 11 March 2009, No de rôle 34284.

16. **As regards your answer to question 41 of the first questionnaire: could you explain what you mean by "infiltration tests"? Please also state which of the possibilities mentioned are facultative and which are mandatory.**

"Infiltration test" refers to "penetration tests", which are a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. Of the measures mentioned in question 41, only the external control by the CNPD is mandatory.

17. **As regards your answer to question 34/44 of the first questionnaire:**

- **Is Luxembourg a party to the European Convention on Mutual Assistance in Criminal Matters?**

  Yes, since 1977.[22]

- **Please provide an answer to the following questions, taken from the first questionnaire (question 34): 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 exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?**

  According to article 6 of the act transposing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union which is applicable for cross-border requests (Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale amended by the loi du 27 October 2010[23]), the responsible authorities are the judicial authorities (the judges, the juge d`instructions and the members of the public prosecution department) and, in case a central authority is required, the director of public prosecution (procureur général d`Etat). Concretely foreign requests for data exchange are centralised via the procureur général d`Etat, the actual providing of the data takes place by the juge d'instruction. A direct access right for foreign state bodies does not exist.

- **Please describe the procedure according to which (ingoing/outgoing) cross-border requests of retained data are handled.**

  According to article 7 (2) of the Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale amended by the loi du 27 October 2010[24],

---

22 Compare http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=030&CM=&DF=&CL=ENG.

23 Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale, Mémorial A – No. 98 of 18 September 2000 amended by the loi du 27 October 2010 Mémorial A – No. 194 from 3 November 2010, accessible at: http://www.legilux.public.lu/leg/a/archives/2010/0194/a194.pdf#page=2.

24 Ibid.

cross-border requests must be directed the director of public prosecution (procureur général d`Etat). He must then inform the juge d`instruction who decides about the authorization of the measure. The juge d`instruction is then obliged to inform the intercepting authority and the director of public prosecution (procureur général d`Etat) within the 96 hours following the request.

In this context one also needs to take note of the following reservation. Article 23 (7) of Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[25] provides that:

"Luxembourg may, when signing the Convention, declare that where personal data are communicated by Luxembourg under this Convention to another Member State, the following applies: Luxembourg may, subject to paragraph 1(c), in the circumstances of a particular case require that unless that Member State concerned has obtained the consent of the data subject, the personal data may only be used for the purposes referred to in paragraph 1(a) and (b) with the prior consent of Luxembourg in respect of proceedings for which Luxembourg could have refused or limited the transmission or use of the personal data in accordance with the provisions of this Convention or the instruments referred to in Article 1.
If, in a particular case, Luxembourg refuses to give its consent to a request from a Member State pursuant to the provisions of paragraph 1, it must give reasons for its decision in writing."

This reservation is transposed by art. 5 of the act transposing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale amended by the loi du 27 October 2010[26]).

---

25 OJ 2000, C-197/1.

26 Loi du 8 août 2000 sur l`entraide judiciaire internationale en matière pénale, Mémorial A – No. 98 from 18 September 2000 amended by the loi du 27 October 2010 Mémorial A – No. 194 from 3 November 2010, accessible at: http://www.legilux.public.lu/leg/a/archives/2010/0194/a194.pdf#page=2.

ANNEX

With a Law of 28 July 2011 Luxembourg completed the transposition of the Directives 2009/136/EC and 2009/140/EC, thereby also amending parts of the Data Protection laws (both the general law and – mainly – the law concerning electronic communications networks and services).[27]

Firstly, the former Art. 41 of Loi 2002 (the general Data Protection Law) is abrogated by the new law. This provision contained the rules on access to stored data used for criminal proceedings according to the requirements set forth by the regulator (ILR). The abrogation of the provision does not, however, mean that the substance of the provision is removed. Instead the relevant parts are to be found in other provisions of the law, e.g. in the new art. 7 para. 5 Loi 2002. An important change is the revision of the procedure for the storage of the data where the formerly foreseen central storing requirements were seen as being a too heavy burden on the providers and a competitive disadvantage in comparison to other EU Member States. This change simplifies the requirements for the storage of data that the authorities might access in the enumerated cases. Further explanation is given in the reasoning for the Law as well as the statement of the CNPD – the latter pointing out the difficulty created originally by mixing up the necessary provisions due to the Telcoms Package of the EU with the Data Retention Directive in the national transposition –, both reprinted in the relevant excerpts below.

Secondly, art. 4 para. 3 lit. b) of Loi 2005 (the specific Electronic Communications Networks and Services Data Protection Law) is amended in a way that describes the access rights in a more general manner.

> Version of art. 4 Loi 2005 before amendment July 2011
> (3) Le paragraphe (2):
> (b) ne s'applique pas aux autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales;
> Version of art. 4 Loi 2005 since amendment July 2011
> «(b) ne s'applique pas aux autorités judiciaires agissant au titre de l'article 67-1 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales;»

---

[27] Mémorial A, n°172 du 10.08.2011, p. 2938, http://www.legilux.public.lu/leg/a/archives/2011/0172/2011A2938A.html; cf. also (forthcoming) IRIS Merlin Database/Newsletter, News Item «LU-Luxembourg : Finalisation de la Transposition de la Directive 2009/136/CE concernant les Communications Electroniques» (Cole).

Version of Art. 41 in consolidated Loi 2002 (as of 2007)

Art. 41. Dispositions spécifiques
(1) (a) Les autorités compétentes visées aux articles 88-1 à 88-4 du Code d'instruction criminelle, et
(b) les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle,
accèdent de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ci-après «ILR») aux données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques ainsi que des services postaux et des fournisseurs de ces services.
(Loi du 27 juillet 2007)
«La centrale des secours d'urgence 112, les centres d'appels d'urgence de la police grand-ducale et la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg accèdent dans les mêmes conditions et modalités que les autorités visées à l'alinéa précédent aux seules données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.»
(2) A ces fins, les opérateurs et les fournisseurs mettent d'office et gratuitement à la disposition de l'ILR les données prescrites au paragraphe (1). Les données doivent être actualisées au moins une fois par jour. L'accès doit être garanti vingt-quatre heures sur vingt-quatre et sept jours sur sept. Un règlement grand-ducal détermine les services de communications électroniques et services postaux pour lesquels les opérateurs et fournisseurs de services doivent mettre à disposition les données ainsi que la nature, le format et les modalités de mise à disposition des données.
(Loi du 27 juillet 2007)
«(3) L'accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d'instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l'article 40 du Code d'Instruction criminelle et aux mesures particulières de secours d'urgence prestées dans le cadre des activités de la centrale des secours d'urgence 112, des centres d'appels d'urgence de la police grand-ducale et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg.»
(4) La procédure est entièrement automatisée suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique.
(Loi du 27 juillet 2007)
«(5) L'autorité de contrôle visée à l'article 17, paragraphe (2) veille au respect du présent article.»

Consequence re. Art. 41 by consolidated Loi 2002 (as of 2011) – Deletion

Loi du 28 juillet 2011 portant modification
1) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques;
2) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel;
3) de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat;
4) du Code de la consommation.

Art. 8. La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel est modifiée comme suit:
1. Le paragraphe (2) de l'article 34 est modifié comme suit: […]
2. L'article 41 (Dispositions spécifiques) est supprimé.

Art. 5. A l'article 7 (Identification de la ligne appelante et de la ligne connectée) il est inséré au paragraphe (5) les lettres (a) et (b) libellées comme suit:
«(a) Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation transmet («push») pour chaque appel à destination d'un de ces numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation.
Aux termes du présent paragraphe on entend par «données disponibles»:
– les données relatives à l'identification: le numéro de téléphone, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, lieu d'établissement de l'abonné et de l'utilisateur pour autant que ce dernier soit identifié ou identifiable; l'indication du caractère public ou non public des données, ainsi que – toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public (données de localisation).
(b) L'Institut luxembourgeois de régulation fixe, en cas de besoin, le format et les modalités techniques de mise à disposition des données visées au paragraphe (5).»
L'actuel paragraphe (5) devient la lettre (c). A la nouvelle lettre (c) les termes «et les données de localisation de l'appelant» sont insérés après «l'identification de la ligne appelante.»

Proposal for Amending Law of July 2011 (accompanying documents)

Projet de Loi No. 6243 (Documents as of 15.2.2011)
Chambre des Deputes
Projet de Loi portant modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Expose des Motifs

L'abrogation de l'article 41 (Dispositions spécifiques) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel s'explique essentiellement par 2 types de difficultés rencontrés lors de la tentative de mise en œuvre pratique du système décrit à l'article 41. L'un tient à la spécificité du système – notamment du fait de devoir gérer le système d'information sans avoir le droit d'accéder aux informations y traitées – et à la complexité de l'architecture du système d'information, l'autre tient à la maintenance du système. La mise en œuvre pratique de l'article 41 aurait en outre généré des coûts exorbitants et disproportionnés par rapport à sa finalité.

Avis de la CNPD (10.11.2010)

Article 7: Identification de la ligne appelante et de la ligne connectée
(et abrogation de l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel)
Le projet de loi se propose d'insérer au paragraphe 5 de l'article 7 de la loi des dispositions assurant que tout fournisseur ou opérateur de téléphonie fixe ou mobile transmet d'office pour chaque appel à destination d'un des numéros d'urgence déterminés par l'ILR les données d'identification et de localisation disponibles.
Ces nouvelles dispositions remplacent aussi bien la dernière phrase de l'article 9 paragraphe (1) dont la suppression par la loi du 24 juillet 2010 avait donné lieu à un regrettable vide juridique et l'article 41 actuel de la loi modifiée du 2 août 2002 qui poursuivaient le même objectif, à savoir garantir en cas d'appel d'un numéro d'urgence de la Police grand-ducale ou des services de secours (112, opéré par la Protection civile et le service d'incendie et de sauvetage de la Ville de Luxembourg) l'accès de plein droit des autorités policières respectivement des services de secours d'urgence à toutes les données d'identification et de localisation disponibles des personnes à l'origine de l'appel (de détresse ou de signalement).

Elles sont parfaitement adaptées aux yeux de la Commission nationale pour résoudre la difficulté soulevée à juste titre par le Ministre de l'Intérieur et de la Grande Région et répondre à son souhait de voir rétablir le fondement légal de l'accès aux données permettant à la Police grand-ducale, au Central des Secours d'Urgence et au Central du service d'incendie et d'ambulance de la Ville de Luxembourg d'identifier et de localiser les personnes dont émane l'appel.
Notre Commission ne partage en revanche pas l'avis exprimé par Monsieur le Directeur général de la Police grand-ducale que le système prévu aux termes de l'article 41 de la loi modifiée du 2 août 2002 sur la protection des données et dont la mise en oeuvre n'a jamais abouti pour des raisons techniques au Luxembourg, serait nécessaire ou préférable à celui prévu par le projet de loi.
Le législateur de 2002 avait retenu à l'article 41 une solution centralisée dont il s'est avéré par la suite que seul un Etat membre, à savoir les Pays-Bas, l'a choisie et effectivement mise en service. Les conditions de sécurité nécessaires pour protéger une banque de données centralisée ont constitué, semble-t-il, un obstacle empêchant sa réalisation opérationnelle par l'ILR. Dans tous les autres pays de l'Union Européenne l'accès des autorités policières et judiciaires à ces données s'effectue de façon décentralisée directement auprès des opérateurs de réseaux de téléphonie fixe ou mobile.
Dans son avis du 26 avril 2010 (Délibération No 85/2010) relatif au projet de loi No 6113 relatif à la conservation des données relatives aux communications électroniques, notre Commission nationale s'était exprimée clairement en défaveur de la mise en place d'un stockage centralisé des données de trafic provenant de l'ensemble des opérateurs de réseaux et fournisseurs de services de communications électroniques (comme le CIOT aux Pays-Bas) pour l'accès des autorités judiciaires agissant au titre de l'article 67-1 du Code d'Instruction criminelle et de celles compétentes en vertu des articles 88-1 à 88-4 pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche et la constatation et la poursuite des infractions pénales emportant une prise minimale prévue par la loi du 24 juillet 2010. Elle avait été suivie sur ce point par le législateur.
La modification de l'article 41 (extension aux données de localisation) envisagée dans le courrier prémentionné du Directeur général de la Police grand-ducale conduirait à une confusion non souhaitable entre les dispositions légales ayant pour objet la transposition de la directive 2006/24/CE du 15 mars 2006 sur la conservation des données générées et traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et celles répondant au besoin spécifiquement visé dans le courrier de Monsieur le Ministre de l'Intérieur et de la Grande Région. Les nouvelles dispositions prévues au projet de loi répondent à ce besoin.
Notre Commission nationale y marque donc son accord et approuve l'abrogation proposée de l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.