The cooperation of Internet and other service providers with judicial authorities

National report on Luxembourg

Prevention of and Fight against Crime Programme of the European Union, ISEC Programme

Project Towards Polish Cybercrime Centre of Excellence

Vanessa FRANSSEN[1] and Katalin LIGETI[2]
University of Luxembourg[3]

Co-funded by the Prevention of and Fight against Crime Programme of the European Union

Introductory remarks

Luxembourg likes to praise itself for its first-class information and communication technologies (ICT) infrastructures as well as telecommunications networks.[4] The development of the information society has been a key priority in Luxembourg for a number of years.[5] To this end, the country has created a favourable economic climate for the ICT sector and electronic commerce. Its applicable legal framework is well developed, with a strong emphasis on privacy protection. In addition to local and regional ICT businesses, Luxembourg hosts several data centres as well as the European headquarters of some global players of the IT services industry and electronic commerce (e.g. Skype and Amazon).[6]

The Luxembourgish regulatory framework regarding the telecommunications and ICT sector consists, generally speaking, of two sets of legal instruments: legal instruments relating to the business and technical elements of electronic communications and e-commerce on the one hand, and legislation relating to the protection of privacy and personal data in the field of electronic communications on the other. These regulations are strongly influenced by the existing EU legal framework. Furthermore, the (compulsory) cooperation of telecommunications operators and providers with judicial authorities in the context of a criminal investigation is regulated by the Code of Criminal Procedure ('*le Code d'instruction criminelle*').

Luxembourg's eagerness to stimulate the ICT and e-commerce sector, as well as its well-established financial sector, obviously make the country particularly prone to cyber criminality. That being said, it took Luxembourg until July 2014 to finally approve the Budapest Convention on Cybercrime, and to adjust its national legislation accordingly. With respect to child pornography, Luxembourg has implemented the Directive of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography in 2013.

---

[1] Dr Vanessa FRANSSEN is a postdoctoral researcher at the University of Luxembourg and a senior affiliated researcher at the Institute of Criminal Law of the KU Leuven.
[2] Prof. Dr Katalin LIGETI is a professor of criminal law at the University of Luxembourg.
[3] The authors would like to thank Olivier DINET and Dr Anna DAMASKOU for their valuable assistance in preparing this report.
[4] See e.g. http://www.luxembourg.public.lu/fr/economie/economie-numerique/nouvelles-tech/index.html . See also L. FUNCK, "Chapter 17: Luxembourg", *Technology, Media and Telecommunications Review* 2014, (250) 251-252.
[5] See e.g. https://www.gouvernement.lu/3797584/communications-electroniques . See also L. FUNCK, "Chapter 17: Luxembourg", *Technology, Media and Telecommunications Review* 2014, (250) 259.
[6] http://www.luxembourg.public.lu/fr/economie/economie-numerique/nouvelles-tech/index.html .

In addition to a quite well-developed legal framework, Luxembourg has launched initiatives to enhance awareness about the risks linked to ICT and to contribute to a more secure use of those technologies. In this respect, it is noteworthy to mention, for instance, the creation of a national website called 'BEE SECURE',[7] which offers citizens an online hotline to report illegal content anonymously,[8] and Luxembourg's membership of the international INHOPE network, acting against various illegal activities on the Internet.[9]

1. How providers of publicly available telecommunication technologies are classified in the legal system of your country?

By means of a *preliminary observation*, it is noteworthy that the general term *service provider* is used in several Luxembourgish laws relating to telecommunications technologies and electronic services. However, depending on the legislation in question, the meaning of the term differs. To a large extent, the differences are due to the underlying European legal instruments. Hence, in order to determine the scope of application of a certain law, one should always start by checking which kinds of providers are covered.

The *Law of 30 May 2005* concerning the protection of privacy relating to the processing of personal data in the electronic communications sector[10] transposes, amongst others,[11] Framework Directive 2002/21/EC[12] and the Data Retention Directive of 2006.[13] In particular, the 2005 Law contains the obligation for certain operators and service providers to keep traffic and location data. The 2005 Law applies to 'the processing of (…) personal data in the context of the supply of publicly available electronic communications services over the public communications networks.'[14] In line with the definitions laid down in Framework Directive 2002/21/EC, *public communication networks* are defined as 'electronic communications network[s] used wholly or mainly for the provision of publicly available electronic communications services.'[15] The provider of such a public communications network is referred to as the *operator*.[16] *Electronic communications networks* are defined as:

> '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

[7] https://www.bee-secure.lu/ .
[8] https://stopline.bee-secure.lu/ .
[9] http://www.inhope.org/gns/home.aspx .
[10] *Mémorial* A No 73, 7 June 2005. Coordinated version published in *Mémorial* A No 172, 10 August 2002.
[11] To be complete, the Law of 30 May 2005 transposes, consecutively, Directives 1995/46/EC, 2002/58/EC, 2006/24/EC and 2009/136/EC. Recently, it has also been amended by the Law of 18 July 2014, approving the 2001 Council of Europe Convention on Cybercrime (hereinafter: the Budapest Convention), *Mémorial* A No 133, 25 July 2014, republished in *Mémorial* A No157, 12 August 2014.
[12] In full: Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, *OJ* L 108, 24 April 2002, 33.
[13] In full : Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105, 13 April 2006, 54. This Directive was invalided by the EU Court of Justice on 8 April 2014 (CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*, 8 April 2014).
[14] Article 1 of the Law 30 May 2005. Unlike Article 1 of the Data Retention Directive, the Luxembourgish Law does not include an 'or' between 'publicly available electronic communications services' and 'of public communications networks.' The French text of the Law states the following: 'les dispositions suivantes s'appliquent spécifiquement au traitement de ces données à caractère personnel *dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics*.' (italics added)
[15] Article 2 (j) of the Law of 30 May 2005; *cf.* Article 2 (d) of Framework Directive 2002/21/EC.
[16] Article 2 (j) of the Law of 30 May 2005.

conveyed.'[17]

The term *service provider* ('*fournisseur de services*') relates to providers offering an *electronic communications service*. The latter is defined as:

> 'a service normally provided for remuneration, which consists wholly or mainly in the conveyance of signals on electronic communication networks, including telecommunications services and transmission services in networks used for radio broadcasting, *but which 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*.'[18]

By contrast, Article 1 of the *Law of 14 August 2000* on electronic commerce,[19] implementing the Directive on Electronic Commerce,[20] defines *information society services* as 'any service normally provided for remuneration,[21] at a distance via an electronic means and at the individual request of a recipient of services.'[22] The Law further defines the meaning of 'from a distance,' 'via an electronic means' and 'at the individual request of a recipient of services'. Unlike the notion of electronic communication services (*supra*), the term information society services is thus defined in a less technical and more functional way. With respect to these information society services, the term *service providers* ('*prestataires*') extends to any natural or legal person[23] providing Internet access or simply transmit information in a communication network ('mere conduit'),[24] proceeding to the automatic, intermediate and temporary storage of such information ('caching'; e.g. proxy servers)[25] and storing the information provided by a recipient of the service ('hosting'; e.g. Facebook, Twitter, Flickr or YouTube).[26]

A similar distinction between electronic communications services and information society services is made by the *Law of 27 February 2011* on electronic communications networks and services.[27] This Law defines a public communication network as 'an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services *which enables the transmission of information between the end points of the network*.'[28] The term *information society services* is defined in the same way as in the aforementioned Law of 14 August 2000, but it is added that radio and television broadcasting services, as defined by the legislation on electronic media, are excluded from the scope of information society services.[29]

In sum, in line with the existing EU legal framework, Luxembourgish law makes a distinction between providers of information society services (ISPs) and providers of electronic communications services (including IAPs). The distinction between both types of service providers becomes

---

[17] Article 2 (i) of the Law of 30 May 2005; *cf.* Article 2 (a) of Framework Directive 2002/21/EC.
[18] Article 2 (k) of the Law of 30 May 2005, italics added; *cf.* Article 2 (c) of Framework Directive 2002/21/EC.
[19] *Mémorial* A No 96, 8 September 2000. This Law was amended by the Law of 2 April 2014 (*Mémorial* A No 64, 22 April 2014).
[20] In full: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *OJ* L 178, 17 July 2000, 1.
[21] According to the EU Court of Justice, information society services 'covers the provision of online information services for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website.' See CJEU, Case C-291/13, *Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and Others*, 11 September 2014, para. 30.
[22] Article 1, para. 1 of the Law of 14 August 2000.
[23] Article 1, para. 2 of the Law of 14 August 2000. *Cf.* Article 2 (b) Directive on Electronic Commerce.
[24] Article 60 of the Law of 14 August 2000.
[25] Article 61 of the Law of 14 August 2000.
[26] Article 62 of the Law of 14 August 2000.
[27] *Mémorial* A No 43, 8 March 2011. This Law repeals the Law of 30 May 2005 on electronic communications networks and services (Article 84 Law of 27 February 2011).
[28] Article 2 (25) of the Law of 27 February 2011, italics added.
[29] Article 2 (28) of the Law of 27 February 2011.

particularly relevant in light of their respective data retention and other legal obligations (*infra*, sub question 2).

2. What are the regulations concerning data retention by IAPs (i.e. providers of publicly available electronic communications services or of public communications networks) and ISPs (i.e. providers of information society services)?

Introductory remarks on the scope of application of the data retention legislation

As explained *supra*, sub question 1, the *Law of 30 May 2005* implements the 2006 Data Retention Directive and applies 'specifically to the processing of (…) personal data in the context of the supply of publicly available electronic communications services over the public communications networks.'[30] Information society services 'which do are not consist wholly or mainly in the transmission of signals by means of electronic communications networks' are excluded from the scope of application of this Law. In other words, the data retention obligations imposed by the 2005 Law only apply to service providers of electronic communications services, including IAPs and some ISPs, to the extent that they offer services which consist entirely or mainly in the transmission of signals. ISPs hosting content are, however, excluded.

Interestingly, certain authors argue that the data retention obligations imposed by this Law (which will be discussed in more detail *infra*) are also applicable to *intermediary service providers*, as defined by the Law of 14 August 2000 on electronic commerce (*supra*, sub question 1).[31] This would imply that providers of information society services would also be impacted by the data retention obligations of the Law of 30 May 2005.[32] Such a broad understanding of the notion *service provider* would probably be more in line with the definition used in the Budapest Convention,[33] including:

> '(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
>
> (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.'

Unlike the Luxembourgish definition of service providers of electronic communications services which is based on the criterion of *transmission of signals*, the term *service provider* under the Budapest Convention indeed applies to any entity providing a service to communicate *by means of a computer system*, or to process or store data related to such communication. Nevertheless, it is highly questionable whether the foregoing broad interpretation of the service providers covered by the Law of 30 May 2005 will be accepted by the Luxembourgish courts, considering the wording of Article 1 and the definitions laid down in Article 2 (k) of that Law, which mirror the existing EU legal framework.

Furthermore, it is noteworthy that the 2005 Law will be amended in the near future, as described *infra*, sub question 12, in order to meet the requirements of the CJEU in *Digital Rights Ireland Ltd*.[34]

Data retention obligations

[30] Article 1 of the Law of 30 May 2005.
[31] M. BRAUN, "La ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg", *JT Luxembourg* 2014, (121) 129. See also T. REISCH, *Internet et les nouvelles technologies de la communication face au droit luxembourgeois*, Luxembourg, Mike Koedinger Editions, 2008, 78, see also 60-63.
[32] M. BRAUN, *op. cit.*, 2014, 130.
[33] The Convention was signed by Luxembourg on 28 January 2003, ratified on 16 October 2014 and implemented by the Law of 18 July 2014 (*Mémorial* A No 133, 25 July 2014, republished in *Mémorial* A No157, 12 August 2014).
[34] CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*, 8 April 2014.

Turning to the contents of the Law of 30 May 2005, one should distinguish between the obligation to retain *traffic data*,[35] regulated by Article 5 of the 2005 Law, and the retention of *location data other than traffic data*,[36] regulated by Article 9. Apart from their different scope of application *ratione materiae*, these provisions are drafted in a fairly similar way. Briefly summarized, they provide that service providers and operators processing traffic and/or location data should retain the data for a period of 6 months (previously 12 months) for the purpose of the investigation, detection and prosecution of serious criminal offences, in case judicial authorities would need those data. During the 6-month period, the data may be accessible only by the authorities for serious reasons enlisted in the Article in name or by the authorities competent for litigation regarding interconnection and billing. After the 6-month period, the service providers and operators must delete the data in name and render them anonymous.

More specifically, Article 5 of the Law of 30 May 2005 provides the following with respect to the retention of *traffic data*:

> '(1) (a) For the purposes of the investigation, detection and prosecution of criminal offences, subject to a criminal penalty or a correctional penalty[37] of maximum one year or more, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing or generating traffic data in the context of the supply of services must retain such data for a period of 6 months from the date of the communication. The obligation to retain data shall include the retention of the data relating to unsuccessful call attempts where those data are generated or processed and stored (as regards telephony data) or logged (as regards Internet data) in the process of supplying the communication services concerned. A Grand-Ducal Regulation ['*un Règlement grand-ducal*'] shall determine the categories of traffic data which may be used for the investigation, detection and prosecution of criminal offences referred to above. This Regulation may also determine the forms and modalities according to which the data concerned are to be made available to the judicial authorities.
>
> (b) Upon the expiry of the retention period provided for in (a), the service provider or operator shall be required to erase the traffic data relating to subscribers and users, or to render them anonymous.
>
> (2) Every service provider or operator processing traffic data relating to subscribers or users shall be required to take all necessary steps to ensure the retention of such data for the period provided for in paragraph (1) (a), in such a way as to make it impossible for anyone to access the data in question once they are no longer needed for the transmission of a communication or for the processing pursuant to paragraphs (3) and (4), with the exception of access which is:
>
> - ordered by judicial authorities acting in the context of their legal powers,[38] or by the authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard national security, defence, public security and for the prevention, investigation, detection and prosecution of criminal offences referred to in paragraph (1) (a), or

[35] Traffic data are defined by Article 2 (e) of the Law 30 May 2005.
[36] Location data are defined by Article 2 (f) of the Law 30 May 2005.
[37] It should be noted that the Luxembourgish system follows the old French distinction between – in decreasing order of seriousness – crimes ('*les crimes*'), misdemeanours ('*les délits*') and petty offences ('*les contraventions*'). The first category of offences are punishable by a 'criminal' penalty (which is a somewhat confusing translation of '*peine criminelle*'), the second by a 'correctional' penalty ('*peine correctionnelle*') and the third category by a 'police' penalty (once more a misleading translation of '*peine de police*', because this police penalty is still imposed by a court).
[38] Before the amendment by the Law of 18 July 2014 approving the Budapest Convention, reference was only made to the investigative powers under Article 67-1 of the Code of Criminal Procedure (*infra*).

- requested by the competent bodies with a view to settling disputes, in particular interconnection or billing disputes.

(…)

(5) The processing of traffic data in the context of the activities referred to in paragraphs (1) to (4) shall be restricted to persons acting under the authority of the service provider or operator and handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service. It must be restricted to what is necessary for the purposes of such activities.

(6) Whoever violates the provisions of paragraphs (1) to (5) of the present article is punishable by a prison sentence of eight days up to one year and by a fine of 251 up to 125,000 euros or by one of these penalties only. The court of competent jurisdiction can cease the acts contrary to the provisions of the present article, and imposes a monetary penalty in case of non-compliance, the maximum of which is set by the court.'

Article 9 states the following with respect to *location data other than traffic data*:

'(1) (a) For the purposes of the investigation, detection and prosecution of criminal offences, subject to a criminal penalty or a correctional penalty of a maximum of one year or more, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing or generating location data other than traffic data must retain such data for a period of 6 months from the date of the communication. The obligation to retain data shall include the retention of the data relating to unsuccessful call attempts where those data are generated or processed and stored (as regards telephony data) or logged (as regards Internet data) in the process of supplying the communication services concerned. For the purpose of this paragraph, only one single location information is needed per communication or call. A Grand-Ducal Regulation shall determine the categories of location data other than traffic data which may be used for the investigation, detection and prosecution of criminal offences referred to above. This Regulation may also determine the forms and modalities according to which the data concerned are to be made available to the judicial authorities.

(b) Upon the expiration of the retention period provided for in (a), the service provider or operator shall be required to erase the location data other than traffic data which relate to subscribers and users, or to render them anonymous.

(2) Every service provider or operator processing location data other than traffic data relating to subscribers and users shall be required to take all necessary steps to ensure the retention of such data for the period provided for in paragraph (1) (a), in such a way as to make it impossible for anyone to access the data in question with the exception of access which is ordered by judicial authorities acting in the context of their legal powers,[39] or by the authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard national security, defence, public security and for the prevention, investigation, detection and prosecution of criminal offences referred to in paragraph (1) (a).

(3) Every service provider or operator may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or if the subscriber or user concerned has given his/her consent thereto, to the extent and for the duration necessary for the supply of a value-added service and subject to the provisions of paragraphs (2), (4) and

[39] Once again, before the amendment by the Law of 18 July 2014, reference was only made to the investigative powers under Article 67-1 of the Code of Criminal Procedure (*infra*, sub question 6).

(5).

(4) The service provider and, where appropriate, the operator shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the added value service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time. Where the subscriber or user has given his/her consent for the processing of location data other than traffic data, he/she must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

(5) The processing of location data other than traffic data in the case of the activities referred to in paragraphs 1 to 4 shall be restricted to persons acting under the authority of the service provider or operator or of the third party providing the value-added service, and must be restricted to what is necessary for such activities.

(6) Whoever violates the provisions of paragraphs (1) to (5) of the present article is punishable by a prison sentence of eight days up to one year and by a fine of 251 up to 125,000 euros or by one of these penalties only. The court of competent jurisdiction can cease the acts contrary to the provisions of the present article, and imposes a monetary penalty in case of non-compliance, the maximum of which is set by the court.'

The Grand-Ducal Regulation referred to in Articles 5 and 9 of the Law of 30 May 2005 is the Regulation of 24 July 2010 determining the categories of personal data generated or processed in the framework of the provision of services of electronic communications or networks of public communications.[40] Article 3 of this Regulation sets forth which data have to be retained (*infra*, sub question 4).

3. Are there any traffic data related to technologies such as Facebook, blogs or other information society services covered by your national legislation?

The provisions on the retention of traffic data can be found in the Law of 30 May 2005 and the Regulation of 24 July 2010. As discussed above (*supra*, question 2), the Law of 30 May 2005 applies to all service providers offering electronic communication services. This Law does not apply to 'information society services which do not consist wholly or mainly in the transmission of signals to electronic communications networks.'[41] Moreover, services 'providing, or exercising editorial control over, content transmitted using electronic communications networks and services' are excluded as well.[42] The foregoing seems to imply that traffic data relating to services offered by ISPs which only host content provided by a recipient of the service (e.g. Facebook or Twitter) do not have to be kept.

Nevertheless, despite the clear wording of the 2005 Law, it is argued by some authors that the data retention obligations included in that Law apply to all service providers, including intermediary service providers which only transmit or host information provided by a recipient of the service (*supra*, question 2).[43] Whether such broad interpretation will be accepted by the Luxembourgish courts, remains to be seen.

[40] *Mémorial* A No 73, 7 June 2005.
[41] Article 2 (k) of the Law of 30 May 2005.
[42] Article 2 (k) of the Law of 30 May 2005.
[43] M. BRAUN, *op. cit.*, 2014, 130.

In light of the recent case law of the CJEU, one may wonder though whether the current distinction upon which the data retention obligations are based should not be revised.[44]

4. What data are kept by IAPs and ISPs?

As indicated above (sub question 2), the Regulation of 24 July 2010 determines which data are to be kept by the service providers covered by the Law of 30 May 2005. As provided by Article 1 of the Regulation, the data retention obligation extends to *traffic data* and *location data other than traffic data*, with regard to both natural and legal persons. By contrast, the Regulation excludes the retention of *content data* relating to electronic communications, and in particular the content data consulted by means of an electronic communications network.[45] In this respect, the Regulation corresponds to Article 5 (2) of the 2006 Data Retention Directive. Yet, more surprisingly, *data concerning unconnected calls* are also explicitly excluded,[46] even though this seems to be in contradiction with the obligation to keep data relating to unsuccessful call attempts as set forth by Articles 5 (1) and 9 (1) of the Law of 30 May 2005, in conformity with Article 3 (2) of the 2006 Data Retention Directive.

With respect to *traffic data* and *location data other than traffic data*, Article 3 of Regulation of 24 July 2010 determines which specific data are to be kept. This provision is a mere copy of Article 5 (1) of the 2006 Data Retention Directive. Briefly summarized, Article 3 of the Regulation covers the following categories of data:

a. data necessary to trace and identify the source of a communication;

b. data necessary to identify the destination of a communication;

c. data necessary to identify the date, time and duration of a communication;

d. data necessary to identify the type of communication;

e. data necessary to identify users' communication equipment; and

f. data necessary to identify the location of the mobile communication equipment.

5. What are the legal regulations enabling law enforcement and judicial authorities to obtain data from IAP, ISP with particular stress on social networking sites?

The main regulations in this respect can be found in:

- the *Law of 2 August 2002* concerning the protection of persons with regard to the processing of personal data,[47] implementing Directive 95/46/EC. This Law creates the general legal framework for the processing of personal data in Luxembourg and has a broad scope of application, including also the processing of data for the purpose of detecting and prosecuting criminal offences.[48]
- the *Law of 30 May 2005* concerning the protection of privacy relating to the processing of personal data in the electronic communications sector;
- the *Code of criminal procedure* (as amended by the Law of 18 July 2014 approving the Budapest Convention);

[44] See in particular CJEU, Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014. In this case the Court ruled that Google's search engine is 'processing data' because it collects, stores and discloses personal data (para. 28) and that it is playing the role of a 'controller' of personal data, even though 'it does not exercise control over the personal data published on the web pages of third parties' (para. 34). This broad judicial interpretation of the definitions used in Directive 95/46/EC also seems to affect the 2006 Data Retention Directive, as Article 2 (1) of the latter Directive explicitly declares the definitions of the former applicable.
[45] Article 1 of the Regulation of 24 July 2010. See also Article 3 (2) of the same Regulation.
[46] Article 3 (2) of the Regulation of 24 July 2010.
[47] *Mémorial* A No 91, 13 August 2002. Coordinated version published in *Mémorial* A No 131, 8 August 2007.
[48] Article 3 (1) of the Law of 2 August 2002.

- the *Regulation of 1 December 2008* on technical specifications for the interception of electronic communications, enacted on the basis of *inter alia* the Law of 2 August 2002 and the Law of 30 May 2005;[49]
- the *Regulation of 21 December 2004* determining the services of electronic communications and the postal services, as well as the nature, the format and the modalities of making available data, enacted on the basis of *inter alia* the Law of 2 August 2002.[50]

The content of these regulations will be discussed below, under question 6.

6. What are the legal requirements for an access to traffic data, stored content (e.g. e-mail message) and subscriber's data by LE/judicial authorities from ISPs ?

Confidentiality of communications

The starting point for any access to subscriber data, traffic data or content (whether stored or in the course of transmission) is the *principle of confidentiality of all communications*. In addition to Article 28 of the Constitution, which protects the traditional secrecy of communications by poste or telegrammes, Article 4 of the Law of 30 May 2005 guarantees the confidentiality of communications for which a public network or electronic communications service is used:[51]

> '1. Every service provider operator shall guarantee the confidentiality of *communications conducted by means of a public communications network and publicly available electronic communications services, as well as the confidentiality of the traffic data relating thereto.*
>
> 2. *No person other than the user may listen, intercept, store the communications and the traffic data relating thereto,* or to submit them to any other means of interception or surveillance without the consent of the user concerned.
>
> 3. Paragraph (2):
>
> (a) does not preclude the necessary technical storage for the transmission of a communication, without prejudice to the principle of confidentiality;
>
> (b) *does not apply to the judicial authorities* acting in the context of their legal powers,[52] neither to the authorities competent pursuant by virtue of Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard national security, defence, public security and for the prevention, investigation, detection and prosecution of criminal offences;
>
> (…)
>
> 4. Whoever violates the provisions of the present article is punished with eight days to one year imprisonment and with a fine of 251 to 125,000 euros or with only one of these penalties. The court of competent jurisdiction can cease the acts contrary to the provisions of the present article, and imposes a monetary penalty in case of non-compliance, the maximum of which is set by the court.'[53]

[49] *Mémorial* A No 188, 18 December 2008.
[50] *Mémorial* A No 209, 30 December 2004.
[51] *Cf.* Article 5 (1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201, 31 July 2002, 37.
[52] Until the amendment by the Law of 18 July 2014 approving the Budapest Convention, reference was only made to the investigative powers under Article 67-1 of the Code of Criminal Procedure (*infra*).
[53] Italics added.

Similarly, Article 4 (1) of the Law of 27 February 2011 on electronic communications networks and services (*supra*, sub question 1) states that all businesses offering electronic communications services, including their staff, have to respect the secrecy of communications.

It should be emphasized, though, that the aforementioned Article 4 of the Law of 30 May 2005 only applies to communications transmitted via a public communications network and via publicly available electronic communications services. Therefore, the foregoing provision is supplemented by Article 509-3, paragraph 2 of the Criminal Code,[54] which also applies to the transmission of data via internal networks, data processing systems and automatic data transmission systems.[55] Article 509-3, paragraph 2 of the Criminal Code, which was introduced by the Law of 18 July 2014 approving the Budapest Convention, states:

> 'Whoever intercepts, intentionally and in violation of another person's rights, data during non-public transmissions towards, from or inside a processing system or an automatic data transmission system shall be punishable by the same penalties' as in paragraph 1, namely with a prison sentence of three months up to three years and/or a fine of 1,250 up to 12,500 euros.

However, this offence does not apply to judicial authorities acting on the basis of Articles 67-1 and 88-1 until 88-4 Code of Criminal Procedure (*infra*).[56]

The central concern of privacy and confidentiality also transpires from the obligation of service providers to guarantee the secure processing of personal data in the context of their services and to make sure that only authorized persons are given access to those data.[57] Moreover, they should store the traffic data and location data in a secure manner[58] (*supra*, question 1) and should delete the stored data after the expiry of the data retention period of 6 months (see also pending Bill No 6763, *infra*, sub question 12).

More in general, the Law of 2 August 2002 only allows for the processing of personal data if such processing is necessary for the 'controller' (in the meaning of Directive 95/46/EC)[59] to meet a legal obligation.[60] In particular, the processing of data in the context of criminal investigations and criminal prosecutions must comply with the provisions laid down in the Code of Criminal Procedure.[61] Non-compliance with the foregoing provisions of the Law of 2 August 2002 is punishable by a prison sentence of eight days up to one year and by a fine of 251 up to 125,000 euros or by one of these penalties only.[62]

---

[54] This paragraph was introduced by the Law of 18 July 2014 approving the Budapest Convention.

[55] M. BRAUN, *op. cit.*, 2014, 127.

[56] M. BRAUN, *op. cit.*, 2014, 127. However, when acting outside the scope of their legal competences, law enforcement or judicial authorities could be held liable of the offence of Article 509-3 of the Criminal Code. *Cf.* CSJ corr. 27 June 2012, 342/12 X, *Receuil de Jurisprudence pénale* 2014, 952, convicting a police officer for consulting other persons' data kept by the State outside the scope of his official police tasks.

[57] Article 3 (1), paras 1 and 2 of the Law of 30 May 2005.

[58] Articles 5 (2) and 9 (2) of the Law of 30 May 2005.

[59] Article 2 (d) of this Directive defines the controller as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.' This notion is interpreted broadly by the Luxembourgish courts. See e.g. CSJ corr. 27 June 2012, 342/12 X, *Receuil de Jurisprudence pénale* 2014, 952 ('Le responsable du traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaire relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités du traitement et les moyens pour y parvenir. Il s'agit de celui qui prend l'initiative et qui dispose du pouvoir décisionnel en relation avec le traitement. (…) la loi de 2002 a vocation à s'appliquer en l'espèce aux agissements du prévenu puisqu'elle a un champ d'application très large, qu'elle concerne toutes les personnes physiques, les personnes morales et l'Etat qui effectuent un traitement de données à caractère personnel'). See also *supra*, CJEU, Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.

[60] Article 5 (1) (a) of the Law of 2 August 2002.

[61] Article 8 (1) of the Law of 2 August 2002.

[6262] Articles 5 (2) and 8 (4) of the Law of 2 August 2002.

In the following paragraphs, we will discuss in more detail the legal requirements for the access of judicial authorities to, respectively, subscriber and user data, traffic data, stored content and the interception of content while being transmitted.

Subscriber and user data

Generally speaking, information identifying subscribers and users of electronic (as well as postal) communications services shall be passed on by the operators and service providers to the *Institut luxembourgeois de régulation* (hereinafter: the Institute).[63]

Subsequently, all requests regarding information on subscribers, users and the services they use, have to be addressed to the above Institute, which will then verify whether the person requesting the information has a right to access such data. More precisely, Article 3 of the Regulation of 21 December 2004 states:

> '1. All requests for access to data relating to subscribers, users and their services are made through the Institute. The latter receives the requests, validates them, renders them anonymous and examines the files made available by the operators and the providers of the respective services.
>
> 2. The validation referred to in paragraph (1) consists in a verification of the applicant's access rights. To this end, the hierarchically superior of the legal authorities and bodies mentioned in Article 41 paragraph (1) of the Law of 2 August 2002 communicates to the Institute a list identifying the persons empowered to enforce the requested access rights. Only the requests for which the requestor has a right of access allow for an examination of the files of the operators and service providers.
>
> 3. In order to render the requests anonymous, the Institute removes all information concerning the identity of the requestor before every examination of files made available by the operators and service providers.
>
> 4. The Institute gathers the responses emanating from the examination of the files made available by the operators and service providers and transmits them to the initial requestor in a synthetized manner.'

Even the judicial authorities acting on the basis of their competences laid down in the Code of Criminal Procedure, which will be further discussed below, have to pass through the Institute to obtain subscriber and user data of service providers and operators.[64]

Article 4 of the Regulation of 21 December 2004 sets forth which specific data the operators and providers of electronic communications services have to incorporate in the files they transmit to the Institute. With regard to electronic communications services, those files do not only contain *identification data* regarding, for instance, services of public telephony, data transmission and text messaging, but they also encompass *available location data*.[65]

In case of special measures of surveillance and in cases where the offender is caught in the act of committing a crime ('*crime flagrant*') or a misdemeanour ('*délit flagrant*'), judicial authorities can obtain access to all the information contained in the Institute's files. This is provided for by Articles 5 (1) and 6 (1) of the Regulation of 21 December 2004:

> 'Article 5 – Consultation of data
>
> 1. By virtue of their surveillance missions, in accordance with Articles 88-1 to 88-4 of the Code of Criminal Procedure, when the offender is caught in the act of committing a crime, or in the

[63] Article 2 (1) of the Regulation of 21 December 2004.
[64] Article 41 of the Law of 2 August 2002.
[65] Article 4 (3) of the Regulation of 21 December 2004.

context of Article 40 of the Code of Criminal Procedure [referring to cases of '*délit flagrant*'], the persons duly empowered by virtue of Article 3 paragraph 2 of the present Regulation have access to the *information contained in the totality of the files mentioned in Article 4*.'[66]

'Article 6 – Procedure

1. The information communicated by the Institute to the initial requestor on the basis of a request introduced in the context of special measures of surveillance, when the offender is caught in the act of committing a crime, or in the context of Article 40 of the Code of Criminal Procedure includes *all the information resulting from the examination of the files made available by the operators and service providers, as well as the identity of the operators and providers of the respective services*.'[67]

Tracking and localization of telecommunications

As indicated above (sub question 2), the Luxembourgish law on electronic communications services makes a distinction between traffic data concerning subscribers and users (Article 5 of the Law of 30 May 2005) and location data other than traffic data (Article 9 of the Law of 30 May 2005). The Code of Criminal Procedure makes a comparable distinction between the tracking ('*le repérage*') of telecommunications data and the localisation of the origin and destination of telecommunications, yet without establishing a differential legal regime for these data. In order to trace and/or localize telecommunications, the investigating judge and the public prosecutor may require the cooperation of private actors.

First of all, the *investigating judge*, who is in charge of a judicial inquiry (i.e., a type of pre-trial criminal investigation; '*l'instruction préparatoire*') in case of very serious criminal offences, can order the telecommunications operators or service providers to give the following data, as set forth by Article 67-1 (1), (2), (3) 1st sentence and last paragraph of the Code of Criminal Procedure:

'(1) When the investigating judge estimates that there are circumstances which render the tracking of telecommunications or the localization of the origin or the destination of telecommunications necessary for revealing the truth, and if the facts are punishable by a criminal penalty or a correctional penalty of a maximum of one year or more, the investigating judge may undertake the following investigative measures, and request if necessary the technical assistance of *the telecommunications operator and/or the provider of the telecommunications service*:

1. the tracking of information concerning the means of telecommunication from which or towards which the calls are or have been addressed;

2. the localisation of the origin or the destination of telecommunications.

In the cases provided in the paragraph 1, for each telecommunication means, the call data of which are traced or the origin or destination of which are localized, the day, the hour, the duration and, if necessary, the place of the telecommunication shall be indicated and written down in a record.

The investigating judge indicates the factual circumstances of the case which justify the measures in an order giving reasons, which s/he communicates to the public prosecutor.

He specifies the duration of application of the measure, which may not exceed one month from the date of issuance of the order, without prejudice to renewal of the order.

(2) All telecommunications operators and all providers of telecommunications services communicate the requested information as soon as possible.

[66] Italics added.
[67] Italics added.

All persons who, in the context of their profession, have knowledge of the measure or assist in its execution are obliged to safeguard the secrecy. All violations of secrecy are punished in accordance with Article 458 of the Criminal Code.

All persons refusing to offer their technical help to execute the requests provided in this article are punishably by a fine of 100 up to 50,000 euros.

(3) The person of which a telecommunication means has made the object of the measure provided in paragraph 1 is informed of the ordered measure in the course of the investigation and in any case at the latest within twelve months starting from the date of issuance of the order.

(…)

When the measures of tracking of telecommunications ordered by the investigating judge yield no outcome, the obtained data shall be removed from the criminal file and destroyed to the extent that it refers to persons who do not face charges.'[68]

It should be highlighted that the scope of application of the above provision extends to operators and providers of *telecommunications services*. Hence, one will notice a slight disconnect between the scope of this provision and the data retention obligations laid down in the Law of 30 May 2005 (*supra*, sub question 2). Indeed, Article 67-1 of the Code of Criminal Procedure still uses the old terminology which was used before the enactment of the Law of 27 February 2011 on electronic communications networks and services[69] (*supra*, sub question 1). In the former Telecommunications Law of 21 March 1997,[70] telecommunication was defined as 'each transmission, emission or reception of signals, writings, images, sounds or data of any nature, by wire, radio, optical or electromagnetic means.'[71] However, Internet services were also considered to be governed by the 1997 Telecommunications Law.[72] The notion electronic communications services deliberately covers a wider range of services than the old term telecommunications services.[73]

Second, besides the investigating judge, it is also possible for the *public prosecutor* to request an investigating judge to issue such an order in the context of a so-called 'mini-instruction', meaning that the prosecutor is in charge of the pre-trial investigation (called a preliminary investigation or '*l'enquête préliminaire*') but asks the investigating judge for a punctual intervention for a particular coercive investigative measure. In this respect, reference should be made to Article 24-1 of the Code of Criminal Procedure, which is the general provision for the measures which can be ordered on the basis of a mini-instruction and which explicitly refers to the telecommunications measures of Article 67-1 of the Criminal Code :

'(1) With respect to all misdemeanours, the public prosecutor may request that the investigating judge orders a search of private premises, a seizure, the hearing of a witness or an expertise, without having opened a judicial inquiry.

The public prosecutor may proceed in the same manner with regard to the offences provided in articles 196 and 197 of the Criminal Code with regard to the use of the forged documents provided in Article 196 [forgery by a private person], and for the offences provided in articles

[68] Italics added.
[69] As indicated before, the Law of 27 February 2011 repealed the Law of 30 May 2005 on electronic communications networks and services, which was the first law moving away from the old term 'telecommunications'.
[70] *Mémorial* A No 18, 27 March 1997.
[71] Article 2 (26) of the Law of 21 March 1997.
[72] F. FAYOT and L. FUNCK, "Chapter 20: Luxembourg", *Technology, Media and Telecommunications Review* 2011, (252) 258.
[73] F. FAYOT and L. FUNCK, "Chapter 20: Luxembourg", *Technology, Media and Telecommunications Review* 2011, (252) 253-254 and 258.

467, 468 and 469 of the Criminal Code [theft with aggravating circumstances or with violence].[74]

With respect to the offences referred to in the preceding paragraph and the misdemeanours punishable by a correctional penalty of a maximum of one year or more, the public prosecutor may request that the investigating judge orders the measures provided in paragraphs 1 and 2 of Article 67-1, without having opened a judicial inquiry.

The person whose means of telecommunication has made the object of the measure provided in paragraph 1 of Article 67-1 is informed of the ordered measure in the same course of preliminary investigation and in any case in twelve months at the latest commencing from the date of issuance of the order.

When the measures of tracking of telecommunications as ordered by the investigating judge yield no outcome, the obtained data shall be removed from the preliminary investigation file and destroyed to the extent that it refers to persons who are not included in the preliminary investigation.

(…)

(3) If the investigating judge returns the file, the persons included in the preliminary investigation are interrogated, prior to the citation or referral by the investigating court ['*la chambre du conseil'*] to the trial court. Before proceeding to the interrogation, the officers and the agents of the judicial police referred to in Article 13 inform the respondent, in writing and with receipt, in a language which the respondent understands, of the right to receive legal assistance and advice, except in cases where it is duly established that this is materially impossible.

(4) The public prosecutor may not proceed to a second request, within the meaning of paragraph 1, within a period of three months after the investigating judge has returned the file to him.

(5) The public prosecutor, as well as any person concerned having a legitimate personal interest can, by simple request, ask for the annulment of an investigative measure or of the measures executing the latter.'[75]

In addition to the tracking and localisation of telecommunications, the Law of 18 July 2014 approving the Budapest Convention introduced the possibility of a *quick freezing of data*, allowing for the expedited preservation of computer data.[76] Undeniably, this measure can be particularly useful in case of volatile digital data. In this respect, Article 48-25 Code of Criminal Procedure states:

> 'When there are reasons to believe that the data stored, processed or transmitted in a system of processing or automatic transmission of data, which are useful for revealing the truth, are susceptible to loss or modification, the public prosecutor or the investigating judge may proceed to the rapid and immediate freezing of the data, for a period not exceeding 90 days.'

The scope of application of this provision extends to all types of electronic data, including traffic data but also content data,[77] which brings us to the next category of data.

Content data

[74] These offences are defined as crimes ('*crimes*') by the Criminal Code.
[75] Italics added.
[76] *Cf.* Articles 16 and 17 of the Budapest Convention.
[77] M. BRAUN, *op. cit.*, 2014, 130-131.

When analysing the legal requirements concerning the access to content data, one should distinguish between the *interception* of data in the course of their transmission and the *seizure of stored data*.

The main provisions relating to the *interception of data* are Articles 88-1 to 88-4 of the Code of Criminal Procedure. These provisions regulate the use of technical equipment for the surveillance and monitoring of *any form of communication* (Article 88-1 and 88-2), with a number of specific procedural rules applicable to offences against the external security of the State, possibly including cyberterrorism (Articles 88-3 and 88-4).

In particular, Article 88-1 states:

> 'The investigating judge can, exceptionally and by means of a decision giving special reasons based on factual elements and with reference to the conditions mentioned hereinafter, order the use of technical means of surveillance and monitoring of *all forms of communication*, if:
>
> a) the criminal prosecution concerns a fact of particular gravity punishable by a criminal penalty or a correctional penalty of a maximum of two years or more; and if (…)
>
> c) ordinary investigative measures appear to be ineffective due to the nature of the facts and the specific circumstances of the case.
>
> The ordered measures shall be lifted as soon as they are no longer necessary. They shall be automatically terminated one month after the date of the issuance of the order. They may, however, be extended each time for a month, yet without the total duration exceeding one year, by an order of the investigating judge which gives reasons and which is approved by the president of the investigating chamber ['*chambre du conseil*'] of the Court of Appeals. The Court of Appeals shall rule within two days from the reception of the order, after having heard the opinion of the public prosecutor general.'[78]

Article 88-2 continues as follows:

> 'The decisions by virtue of which the investigating judge or the president of the investigating chamber of the Court of Appeals ordered the surveillance and the monitoring of telecommunications, as well as the correspondence entrusted to the post, will be notified to the operators of the postal services and telecommunications, which shall execute them without delay.
>
> These decisions and their execution shall be recorded in a special register kept by each operator of postal services and telecommunications.
>
> The registered telecommunications and the correspondences, as well as the data or information obtained by other technical means of surveillance and monitoring on the basis of Article 88-1 shall be delivered sealed and upon receipt to the investigating judge, who will draw up a written record of their release. He shall copy the correspondences which could serve as a basis for a conviction or a discharge and shall include these copies, the recordings, as well as all other data and information in the file. He shall return the documents which he does not consider necessary to seize, to the operators of the postal services, which will send them without delay to the addressee.
>
> When the measures of surveillance and monitoring of communications ordered on the basis of Article 88-1 do not yield any outcome, the copies and the recordings, as well as all other data and information included in the file, shall be destroyed by the investigating judge at the latest twelve months after the order to put an end to the surveillance measures. (…)'

With respect to criminal offences against external security of the Luxembourgish State, Article 88-3, paragraph 1 of the Code of Criminal Procedure states:

[78] Italics added.

> 'The President of the Government can, with the consent of a commission composed of the President of the Supreme Court, the President of the Administrative Court and the President of the District Court of Luxembourg, order the surveillance and the monitoring, using the appropriate technical means, of *all forms of communication* for the purpose of investigating the offences against the external security of the State which one or more authors are attempting to commit, or have committed, or have attempted to commit, if ordinary investigative measures prove to be ineffective due to the nature of the facts and special circumstances of the case.'[79]

More detailed regulations concerning the interception of content data can be found in the Regulation of 1 December 2008 (*supra*, sub question 5), in particular in Articles 4-6.

As regards the seizure of *stored content data*, the existing provisions of the Code of Criminal Procedure were amended last summer, in light of the Budapest Convention. The Luxembourgish law now explicitly encompasses the possibility of seizing all kinds of electronic data.[80] Considering however that such data are volatile, a seizure will usually be preceded by a freezing of data,[81] in accordance with Article 48-25 Code of Criminal Procedure (*supra*, traffic data).

Seizure of content data can be done either by the *judicial police*, informing the public prosecutor, when the offender is caught in the act, or by the *investigating judge* (*infra*).

The first hypothesis, in which the *judicial police* seize the data, is regulated by Article 31 of the Code of Criminal Procedure, stating:

> '(1) In case the offender is caught in the act of committing a crime ['*crime*'], the officer of the judicial police, who is notified immediately by the public prosecutor, goes without delay to the scene of the crime and proceeds to all the useful findings.
>
> (2) He takes care of the preservation of the findings susceptible to disappearance and of all those elements which could contribute to revealing the truth.
>
> (3) *He seizes the objects, documents, data stored, processed or transmitted in a system of processing or of automatic transmission of data and equipment* used for committing the crime or intended to be used for committing the crime and those which form the object of the crime or which appear to be the product of the crime, as well as generally all those which seem useful for revealing the truth, or those of which the use would be likely to harm the smooth conduct of the judicial inquiry, and all those which can be the object of a confiscation or a restitution.'[82]

Furthermore, Article 33 (1) of the Code of Criminal Procedure sets forth that:

> 'If the nature of the crime is such that the evidence sought by the seizure of papers, documents, data stored, processed or transmitted in a system of processing or of automatic transmission of data or other objects possessed by persons who appear to have participated in the crime or to have withheld pieces, data or objects relevant to the criminal events, the officer of the judicial police goes to their residence without delay, in order to proceed to a search, which is reported in a written record, and to seize the relevant objects. This search may take place at any time during the day or night.'

In accordance with Article 40 of the Code of Criminal Procedure, the above provisions are also applicable in case of a '*délit flagrant*'.

[79] Italics added.
[80] M. BRAUN, *op. cit.*, 2014, 131-132.
[81] M. BRAUN, *op. cit.*, 2014, 131.
[82] Italics added.

The second hypothesis, relating to the *seizure of data* when the offender is *not caught red-handed*, is governed by Article 66 of the Code of Criminal Procedure:

> '(1) The investigating judge seizes all the objects, documents, stocks, data stored, processed or transmitted in a system of processing or of automatic transmission of data and any other referred to in Article 31 (3).
>
> (2) The objects, documents, stocks, data and any other seized are listed in written record. If an inventory cannot be drafted on site, they are sealed until they are listed in the inventory, in the presence of persons who have assisted to the search of the private premises.
>
> (3) The seizure of data stored, processed or transmitted in a system of processing or of automatic transmission of data may take place either by a seizure of the equipment or hardware containing those data, or by making a copy of those data in the presence of persons who have assisted to the search. If a copy is made, the investigating judge may order that the data stored, processed or transmitted in a processing system or an automatic data transmission system are definitively erased from the equipment or hardware, provided that the equipment or hardware is located in the Grand Duchy of Luxembourg and that it is not in the possession of the criminal justice authorities, and provided that the possession or usage of the data is illegal or dangerous for the safety of persons or goods. (…)'

Paragraph (4) of the same provision provides for the right of the investigating judge to claim the assistance of a technical expert in case the data are protected or encrypted. Paragraph (5) concerns the written record of the search and seizure procedure, which in principle must be signed by the persons concerned by the search and seizure. Finally, paragraph (6) determines that the seized objects have to be deposited at the court's registry or kept by a person with authority to sequester the objects.

7. Are there any laws, policies or arrangements for the remuneration of costs incurred by ISPs when providing LEAs with requested data?

There is *no general legal framework* relating to the distribution of costs, but in practice the costs for the cooperation with law enforcement and judicial authorities are incurred by the operators and service providers. *However*, with respect to the interception and surveillance of communications, Article 4 (2) of the Law of 27 February 2011 on electronic communications networks and services (*supra*, sub question 1) states explicitly that the operators and providers of electronic communications services provide the competent authorities, automatically and free of charge, with the technical data and means they need to be able to perform their surveillance tasks.

The fact that private actors bear the costs of their cooperation with the public authorities does not give rise to much debate in Luxembourg, at least not as of yet. It is indeed genuinely accepted that these costs are a part of doing business in Luxembourg. That being said, during the legislative debate leading up to the adoption of the Law of 30 May 2005 on electronic communications networks and services,[83] which introduced the aforementioned obligation of operator and service providers to cooperate, free of charge, with the authorities in case of surveillance measures, the Chamber of Commerce did highlight that the free cooperation obligation is not required under EU law and that it would risk to create a competitive disadvantage for operators and businesses in Luxembourg.[84] This argument did, however, not convince the legislator.

[83] As indicated before, this Law was repealed by the Law of 27 February 2011, but the obligation of free cooperation was reincorporated in the 2011 Law.

[84] Avis de la Chambre de Commerce concernant le Projet de loi sur les réseaux et les services de communications électroniques, *Chambre des Députés*, Session 2003-04, No 5185/04, p. 7, available at : http://www.chd.lu/wps/portal/public/RoleEtendu?action=doDocpaDetails&id=5181# .

8. What are the legal regulations concerning taking down and blocking illegal content on the internet before start of criminal proceedings and during criminal proceedings (powers of law enforcement and powers and obligation of service providers), what problems of taking down and blocking could be indicated ?

In 2013 Luxembourg implemented[85] the Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.[86] However, it did not transpose the provisions on blocking illegal content and taking down websites (in particular Article 25 (1) and (2) of the Directive) as it was argued that it was unnecessary.

As far as the *removal* of web pages containing or disseminating child pornography is concerned, the parliamentary documents of the Law of 21 February 2013 pointed out that such a measure was already possible based on the existing provisions regarding seizure.[87] In accordance with Article 31 (3) of the Code of Criminal Procedure (as applicable in 2013), which applies to cases where the offender is caught red-handed, an officer of the judicial police could already seize any object, document or data that has been used or was meant to be used for committing an offence, or that was the object of the offence. Moreover in general, s/he could seize anything that seems useful for discovering the truth or that could harm the criminal investigation. Article 66 (1) of the Code of Criminal Procedure (version 2013) provided the investigating judge with a similar power, regardless of whether s/he is in charge of the investigation (i.e., in case of a judicial inquiry) or whether the seizure is requested by the public prosecutor leading the investigation (i.e., on the basis of a so-called *mini-instruction*, which can be used in most cases, except for the most serious offences) (see also *supra*, sub question 6).

In light of Article 19 of the Budapest Convention,[88] Articles 31 (3) and 66 (1) of the Code of Criminal Procedure were subsequently amended by the Law of 18 July 2014 and now explicitly include the seizure of data stored, processed or transmitted in a computer system (*supra*, sub question 6). In practice such data could, however, already be seized before the amendment of 2014.[89] In addition, it should be emphasized that a seizure of data is only possible if the data are situated in Luxembourg. In practice, this is quite often the case, even in case of foreign ISPs without an office in Luxembourg, because they usually keep a copy of their data on local servers mirroring.[90] If the data are not physically available in the Grand Duchy, the judicial authorities can decide to issue a mutual legal assistance request to their colleagues in the country where the data are (suspected to be) located.

Furthermore, despite the above argument of the legislator in 2013 that an explicit implementation of Article 25 (1) of the 2013 Child Abuse Directive was superfluous considering the existing seizure powers of the judicial authorities, the Law of 18 July 2014 inserted in Article 66 (3) the explicit possibility for the investigating judge to definitively *erase data* which have been copied and seized, *provided that* the device where the data were found is physically located in Luxembourg and has not been seized by the judicial authorities, and *provided also that* the retention or use of the data concerned is illegal or dangerous for the security of persons or goods (*supra*, sub question 6).

---

[85] Law of 21 February 2013, *Mémorial* A No 35, 1 March 2013.

[86] *OJ* L 335, 17 December 2011, 1 (hereinafter : the 2013 Child Abuse Directive).

[87] Projet de loi relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants et portant modification de plusieurs dispositions du Code pénal, *Chambre des Députés*, Session 2011-12, No 6408/00, p. 5, available at : http://www.chd.lu/wps/portal/public/RoleEtendu?action=doDocpaDetails&id=6408# .

[88] In fact, the parliamentary documents also refer to Article 18 of the Budapest Convention, relating to the production order. See Projet de loi portant, i.a., approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, *Chambre des Députés*, Session 2012-13, No 6514/00, p. 13, available at : http://www.chd.lu/wps/portal/public/RoleEtendu?action=doDocpaDetails&id=6514 . However, apart from the possibility to require the technical assistance of an expert in Article 66 (4) (*supra*, sub question 6), Article 66 does not really implement the foregoing Convention provision. Instead, the relevant elements regarding the production order are spread over various other legal provisions (*supra*, sub question 6).

[89] M. BRAUN, *op. cit.*, 2014, 132, with reference to case law of the Luxembourg Court of Appeal, in particular C.A. 9 July 2013, No 375/13, C.A. 16 November 2012, No 752/12 and C.A. 21 December 2011, No 931/11.

[90] M. BRAUN, *op. cit.*, 2014, 132.

The aforementioned possibilities of seizure and erasure of data are *general measures*, meaning that they can be applied to any kind of web pages containing or disseminating illegal content, not just to child pornography.

When it is not possible to remove (data from) a web page, for instance because the data are not located in Luxembourg, there is still the option of *blocking the access* to the web page at hand. When implementing the 2013 Child Abuse Directive, the legislator emphasized that (certain) intermediary service providers already have the obligation to promptly remove illicit information or to make it inaccessible from the moment they have actual knowledge[91] of the illicit activity or information.[92] It should, however, be stressed that, generally speaking, these service providers do not have an obligation to monitor the information they transmit or store, nor do they have a general obligation to search actively for facts or circumstances indicating illicit activities,[93] with the exception of two offences.[94] A global supervisory or monitoring obligation would be unacceptable in light of the confidentiality of communications and the right to privacy.[95] Of course, when judicial authorities order them to monitor a certain activity when this is necessary for the protection of public security or for the purpose of preventing, detecting, investigating or prosecuting criminal offences, they have an obligation to undertake such monitoring.[96] In sum, the legislator concluded there was no need to adopt another express provision for the implementation of Article 25 (2) of the 2013 Child Abuse Directive.[97]

Nevertheless, despite the fact that Luxembourgish judicial authorities have the power to take down a website or to block illegal content, it appears they do not use this power very often in practice. Apparently, the service providers usually take care of such measures themselves, very often triggered by a private complaint on their hotline. This private complaint system seems to be quite effective.

In addition to the foregoing, there is a national online hotline for reporting illegal content, namely the BEE SECURE Stopline,[98] which cooperates with the police in Luxembourg and which is part of the international INHOPE network.

9. Where there any research projects concerning cooperation between LEAs and ISPs/IAPs in fighting cybercrime in your country? If yes, please specify and shortly describe the results. What are the main problems of cooperation?

For the time being, legal research on the cooperation between judicial authorities and ISPs/IAPs from a criminal law perspective is very limited in Luxembourg. We could only retrieve two (policy) reports concerning the fight against cybercrime, one in the context of the Global Alliance against Online Sexual Abuse of Children, and one submitted to CODEXTER, the Council of Europe Committee of Experts on Terrorism, on the use of the Internet for terrorist purposes. Nevertheless, these reports

[91] Some authors argue that service providers should be cautious and make sure to report to the authorities all activities which *appear* to be illicit, in order to avoid later discussions about whether or not they had 'actual knowledge'. T. REISCH, *op. cit.*, 2008, 74.

[92] See in particular Articles 61 e) (concerning ISPs engaged in 'caching') and Article 62 (1) b) (concerning hosting ISPs) of the Law of 14 August 2000 on electronic commerce (*cf. supra*, sub question 1). See Projet de loi portant, i.a., approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, *Chambre des Députés*, Session 2012-13, No 6514/00, p. 13. See also S. LE GOUEFF, *Internet et e-Commerce*, Luxembourg, Editions Portalis, 2003, 190.

[93] Article 63 (1) of the Law of 14 August 2000.

[94] Article 63 (2) of the Law of 14 August 2000 refers to Article 383, para. 2 of the Criminal Code, which apparently no longer exists but used to be inserted in the chapter on sexual offences against minors, and to Article 457-1 of the Criminal Code, encompassing certain hate speech offences.

[95] *Cf.* L. FUNCK, "Chapter 17: Luxembourg", *Technology, Media and Telecommunications Review* 2014, (250) 261; T. REISCH, *op. cit.*, 2008, 75-76.

[96] Article 63 (3) of the Law of 14 August 2000. *Cf. supra* sub question 6, Article 88-1 of the Code of Criminal Procedure.

[97] Projet de loi portant, i.a., approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, *Chambre des Députés*, Session 2012-13, No 6514/00, p. 13.

[98] https://stopline.bee-secure.lu/ .

give some valuable insights into the remaining concerns and gaps in the Luxembourgish system, as the following excerpts illustrate.

- Global Alliance against Child Sexual Abuse Online – 2014 Reporting Form of Luxembourg[99]

> 'The national legislation has not (yet) been adapted in order to regulate the cooperation between law enforcement authorities and the private actors, whose infrastructure and services are used to disseminate child sexual abuse material. In fact, as the cooperation which is based on a non-written gentlemen agreement is excellent and works very well in practice, there was no urgent need for the legislator to intervene in this specific area.
>
> (…)
>
> At the moment we are still trying to find solutions in cooperation with foreign law enforcement authorities and private actors in order to find technological solutions and to improve our computer tools in order to enhance the identification and prosecution of offenders of child sexual abuse.'[100]
>
> 'We have to say that 1-click-hosters represent actually a problem, because it is nearly impossible to effectively take down links, as the content may disappear from national servers, but may reappear elsewhere in the world on servers from the same hoster. This results in bad interpretation of effective notice and bad interpretation of take down times.'[101]

- CODEXTER report on the use of the internet for terrorist purposes in Luxembourg, October 2007[102]:

> 'It is self-evident that in practice, the police – and the State intelligence service as the case may be – are faced with the same technical problems as the corresponding departments of other states, in particular the rapid development of technology, efficient encoding tools, etc.'[103]
>
> 'The law enforcement authorities do not perform any proactive monitoring of the Internet. Only on finding an offence covered by the specific provisions of the Penal Code on terrorism can the investigating judge to whom the case is referred issue an order requiring the access provider or the host of the incriminated site to take blocking and/or closure measures. As regards experiences of collaboration with foreign police departments in this field, the cases dealt with in this way principally concerned national investigations focused on the storage or dissemination of child pornography, whereas it has not yet been possible to acquire experience in measures to block sites preaching terrorism.'[104]
>
> 'There is no formal partnership between the public and the private sectors, although the relevant police departments keep up excellent relations with the service providers and their co-operation is good on the whole.'[105]

10. What problems of cooperation between LEAs/judicial authorities with ISPs/IAPs can be indicated on the base of judicial decisions/judgments?

Case law on this subject is very limited. However there are a couple of pending cases at this very moment which may lead to interesting case law in the near future.

---

[99] Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_luxembourg_en.pdf.

[100] Global Alliance against Child Sexual Abuse Online, Report, p. 2.
[101] Global Alliance against Child Sexual Abuse Online, Report, p. 6.
[102] Available at: http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Luxembourg.pdf.
[103] CODEXTER Report, p. 5, sub question 5.
[104] CODEXTER Report, p. 10, sub question 11.
[105] CODEXTER Report, p. 10, sub question 13.

Based on an interview with a specialized public prosecutor, it appears that the cooperation with service providers other than providers hosting information provided by a recipient of the service (such as Facebook) is quite good in practice, especially if those providers have their headquarters, an office or at least a contact point in Luxembourg. By contrast, the cooperation with service providers located abroad is far from smooth; those providers usually only hand over basic subscriber information.

Furthermore, as pointed out above (*supra*, sub question 6 and 7), if the data processed by such foreign service providers are not stored in Luxembourg (i.e., not even on local servers mirroring), it is impossible for the Luxembourgish judicial authorities to seize the data.

11. What is the effectiveness of investigation and prosecution of illegal content crimes and child abuse on the internet in your country according to available statistical data and research?

There are no publicly available statistical data on the effectiveness of the investigation and prosecution of illegal content crimes and child abuse on the Internet in Luxembourg. But public prosecutors appear to quite positive about the effectivity of their investigations, especially because they can also use valuable information from financial investigations for that purpose.

12. Is there any new legislation prepared or proposed concerning the above mentioned issues? If so, please indicate what are the intended changes and what reasons for them.

There are two pending bills in Parliament which are noteworthy to mention at this point in time.

- Draft Bill No 6763 concerning the amendment of the Code of Criminal Procedure and of the Law of 30 May 2005. This Bill is still pending in Parliament,[106] but includes a number of highly important changes.

Following the CJEU judgment annulling the Data Retention Directive,[107] Luxembourg decided quite quickly to amend its national law. The Ministry of Justice filed on 7 January 2015 a legislative proposal which modifies both the Code of Criminal Procedure and the Law of 30 May 2005. The Bill concerns both traffic data (Article 5 of the Law of 30 May 2005, *supra*, question 2) and location data other than traffic data (Article 9 of the Law of 30 May 2005, *supra*, question 2), and provides for four main amendments to the existing Luxembourgish rules. In particular, the Bill foresees the access of judicial authorities to the retained data on the basis of an *exhaustive and precise list of criminal offences* which are punishable by a prison sentence of at least one year (newly added paragraph 4 to Article 67-1 of the Code of Criminal Procedure). The proposal further provides that the retained data must be *irrevocably and without any delay deleted* at the end of the expiration of the retention period. After the expiration of this period, electronic communication service providers are no longer permitted to store the data in an anonymized form (new Articles 5 (1) (b) and 9 (1) (b) of the Law of 30 May 2005). Moreover, the new Bill *increases the criminal penalties* – in case of non-compliance

---

[106] For an overview of the ongoing legislative process, see http://www.chd.lu/wps/portal/public/!ut/p/b1/04_SjzQ0NTKzNDEzNTPWj9CPykssy0xPLMnMz0vMAfGjzOKNDNzCwtyM3B2DQo2MDBzdTcOCgzzNjA28DYEKIkEKLCyCg9wdfV0tLUOdDDwNnA2DXQOdjAw8jYjTb4ADOBoQ0u_nkZ-bqp8bleNm4aioCAB4d-91/dl4/d5/L0lDU0lKSWdrbUEhIS9JRFJBQUlpQ2dBek15cXchLzRKQ2lEb01OdEJqdEJIZmxDRUEhL1o3XzIwRlZWRjJHQVJVMjIwQUc1VlNSSTYzMFQ3LzA!/?PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_action=doDocpaDetails&id=6763&filter_action=doDocpaDetails&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_displayLink=true&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_numPage=1&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_positionInHistory=&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_display=1&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_EtatDossier=En+cours&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_TypesDeTri=Numero&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_SortOrder=DESC&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_numPageTop=1&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_numPageBottom=1#

[107] CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*, 8 April 2014.

with the Law of 30 May 2005 – to a sentence of six months to two years of imprisonment (new Articles 5 (6) and 9 (6) of the Law of 30 May 2005) and provides that data shall be stored *on the territory of the European Union* (new Article 5-1 (1) of the Law of 30 May 2005). Finally, the Bill announces that a regulation will be adopted in order to lay down detailed enforcement rules to ensure the integrity and confidentiality of the data (new Article 5-1 (2) of the Law of 30 May 2005).

- Draft Bill No 6675, submitted on 2 April 2014, on the establishment of a state intelligence service and amending the Code of Criminal Procedure and of the Law of 30 May 2005. This Bill is still pending in Parliament.[108]

Co-funded by the Prevention of and Fight against Crime Programme of the European Union

[108] For an overview of the ongoing legislative process, see http://www.chd.lu/wps/portal/public/!ut/p/b1/04_SjzQ3NTUzMTQz1I_Qj8pLLMtMTyzJzM9LzAHxo8zijQzcwsLcjNwdg0KNjAwc3U3DgoM8zYwNvEEaIkEKLCyCg9wdfV0tLUOdDDwNnA2DXQOdjAw8jYjTb4ADOBoQ0u_nkZ-bqp8bleNm4aioCABFSVUa/dl4/d5/L0lDU0lKSWdrbUEhIS9JRFJBQUlpQ2dBek15cXchLzRKQ2lEb01OdEJqdEJIZmxDRUEhL1o3XzIwRlZWRjJHQVJVMjIwQUc1VlNSSTYzMFQ3LzA!/?PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_action=doDocpaDetails&id=6675&filter_action=doDocpaDetails&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_displayLink=true&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_numPage=1&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_positionInHistory=&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_display=13&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_numPageTop=1&PC_Z7_20FVVF2GARU220AG5VSRI630T7019404_numPageBottom=1#