DATA RETENTION – THE BELGIAN APPROACH

by

FREDERIK PEERAER*

KEYWORDS
Directive 2006/24/EC, Data Retention, Belgium, Transposition, Belgian approach de lege lata, Belgian approach de lege ferenda, Privacy , Privacy-intrusive, Privacy-invasive

1. INTRODUCTION

1.1 THE PROBLEMATIC NATURE OF DATA RETENTION

"Security, privacy and fundamental rights must be realized together and not at the cost of one another. That is the challenge."[1]

1. Data retention can, for the purpose of this paper, be defined as "*the obligation put on the providers of publicly available electronic communications services or of public communications networks to retain traffic and location data as well as related data necessary to identify the subscriber of user for a certain period*"[2].

Data retention, whenever used as a "*necessary and effective investigative tool for law enforcement*"[3], will necessarily be an interference with the exercise of the right to respect for private life and correspondence as acknowledged

* Frederik.Peeraer@student.ua.ac.be

1 S. Gutwirth, K. De Vries and R. Saelens, "Veiligheid legitimeert niet alle middelen", *Juristenkrant* 24 March 2010, 12.

2 Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, consulted via http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/110530_Evaluation_Report_DRD_EN.pdf, lastly on 25 November 2011 (hereafter: 'Opinion EDPS 2011'), 4, nr.16.

3 Considerans 9, 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* L105, 13 April 2006, 54 (hereafter: 'the Data Retention Directive').

under article 8 of the European Convention of Human Rights (hereafter: 'EHCR') and article 7 of the EU Charter of Fundamental Rights (hereafter: 'EUCFR'). This interference can be justified, according to article 8(2) ECHR and 52(1) EUCFR, if it is provided for by law, serves a legitimate aim and is deemed necessary in a democratic society.

The question arises how this interference can be correctly justified, and subsequently what a fair balance is between law enforcement and privacy and how this balance can be struck. Of course, definite and absolute answers are not to be strived for: instead, I will investigate the actual approach in Belgium of these issues (including some critical remarks) and will try to see whether the balance mentioned above is struck.

Before commencing this investigation, a closer look on the wider regulatory framework seems necessary.

1.2 THE DATA RETENTION DIRECTIVE

2. The most important element in the wider framework is undoubtedly the Data Retention Directive. Apart from this Directive, being very rapidly elaborated[4], the Directives 95/46/EC[5] and 2002/58/EC[6] need to be mentioned as well, as they still are very relevant for this matter.

The Data Retention Directive imposes the obligation for Member States to oblige network and service providers to retain certain data for a period between 6 and 24 months. The access to and use of these data by law enforcement authorities, however intimately connected to the data retention itself, has not been subjected to this (nor any other) Directive.[7] The exact content of the Data Retention Directive will not be dealt with separately: the content of this Directive will be briefly compared to the specific Belgian approach when the scope of the latter is investigated.

1.3 (THE ABSENCE OF A) BELGIAN TRANSPOSITION

3. A single, complete and exhaustive law that transposes the Data Retention

[4] Bill modifying the articles 2, 126 and 145 of the Act of 13 June 2005 relative to electronic communications and the article 90*decies* of the Code of Criminal Procedure, version of 27 August 2009, consulted via http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf, lastly on 25 November 2011 (hereafter: 'Bill modifying diverse articles'), 14.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L281, 23 November 1995, 31.

[6] 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, *OJ* L201, 31 July 2002, 37 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, *OJ* L337, 18 December 2009, 11.

[7] See for a critical approach of the scope of the Directive: Opinion EDPS 2011, *supra* note 2, 6, nrs. 28-31.

Directive has not been issued in Belgium. On the contrary, an amalgam of Acts and Royal Decrees has been issued in order to fulfill the transposition requirement. However, resistance of civil society organizations has been proved efficient to delay the transposition of some articles of the Directive in such a way that some of the transposing legal norms are not yet in force.[8]

4. As a result of the resistance and the choice of modifying existing Acts instead of creating new ones, the actual Belgian transposition is only partial and is scattered among diverse Acts and Royal Decrees, which complicates the general overview of the actual situation.

5. In the following part, the Belgian law will be analyzed both *de lege lata* (2) and *de lege ferenda* (3). In both parts the analysis will be conducted by a detailed investigation of the scope of the relevant legal norms.

2. THE BELGIAN APPROACH *DE LEGE LATA*

6. The actual Belgian situation concerning data retention will be examined in this chapter. Firstly, a general outline of the applicable norms concerning electronic communication and privacy will be given (2.1). Secondly, the situations for the *judicial* (2.2) and the *intelligence- and security* services (2.3) will be explained.[9] Both will be examined separately, since both types of services are governed by specific legal norms.

2.1 GENERAL OUTLINE

7. The general Acts concerning the processing of personal data and electronic communication are the Act of 8 December 1992 relative to the protection of privacy with regard to the processing of personal data[10] (hereafter: 'Privacy Act') and the Act of 13 June 2005 concerning electronic communication[11] (hereafter: 'AEC'). Both remain applicable to data retention and have an impact on the way service providers are allowed to retain and process personal data. According to the Privacy Act, each data

8 *E.g.* propositions of future Acts and Royal Decrees that have been successfully impeded from coming in force: Bill modifying diverse articles, *supra* note 4; Draft of Royal Decree establishing the data to be stored in application of the article 126 of the Act of 13 June 2005, and the conditions and the duration of the storage of these data, version of 14 August 2009, consulted via http://stefaandeclerck.be/files/pdf/dataretentie_KB.pdf, lastly on 25 November 2011 (hereafter: 'Draft of Royal Decree').

9 Except for these services, the Service for Mediation and emergency services also have access to the retained data: see art. 43*bis*, §3, 7° of the Act of 21 March 1991 concerning the reform of certain economic public enterprises, *BS* 27 March 1993 and art. 107 AEC. It would go beyond the scope of this paper to discuss these services as well.

10 *BS* 13 March 1993. The Royal Decree of 13 February 2001 executing the Act of 8 December 1992 relative to the protection of privacy with regard to the processing of personal data, *BS* 13 March 2001 is also to be mentioned.

11 *BS* 20 May 2005.

subject has, *e.g.* the right to access the data that have been processed.[12]

8. Common to both the judicial and intelligence services is the fact that there is *de lege lata no legal obligation* for service providers to retain certain data for a certain period: the specific applicable norms[13] only foresee in a possibility for judicial and intelligence services to demand certain data, which the providers are obliged to communicate if they have these data stored in their systems.[14] The Royal Decree executing art. 126, §2 AEC – which should provide a list of data to be retained and the duration of this retention- has never been issued.[15]

2.2 JUDICIAL SERVICES

2.2.1 SPECIFIC LEGAL NORMS

9. The competence for judicial services to require retained data from service providers has its legal basis in the articles 46*bis* and 88*bis* Code of Criminal Procedure (hereafter: 'CCP'). The Royal Decree of 9 January 2003 contains some extra modalities concerning the legal obligation for services providers to cooperate.

10. According to the first paragraph of the first mentioned article, the *procureur du Roi* (public prosecutor), when dealing with *délits* (misdemeanor of mediocre gravity) or *crimes* has the competence to require the cooperation

[12] Art. 10 Privacy Act. According to the current norms, the subscriber to a connection will have the possibility to control the communication behavior or –data from every user of that connection. The Privacy Commission considers this issue not being sufficiently dealt with: Commission for the Protection of Privacy, Advice concerning the Bill modifying art. 126 of the Act of 13 June 2005 relative to the electronic communication, and concerning the Draft of Royal Decree establishing the data to be stored in application of the article 126 of the Act of 13 June 2005, and the conditions and the duration of the storage of these data (A/08/024), 2 July 2008, nr. 24/2008,consulted via http://www.privacycommission.be/nl/docs/Commission/2008/advies_24_2008.pdf, lastly on 25 November 2011 (hereafter: 'Advice nr. 24/2008'), 10, nr. 23.

[13] Concerning the judicial services, the articles 46*bis*, 88*bis* and 90*quater*, §2 of the Code of Criminal Procedure (hereafter: 'CCP') and the Royal Decree of 9 January 2003 determining the modalities of the legal obligation to cooperate in case of judicial demands concerning electronic communications, *BS* 10 February 2003, as amended by the Royal Decree of 8 February 2011, *BS* 10 February 2011 form the actual basis of this obligation to cooperate (hereafter: 'Royal Decree 9 January 2003'); concerning the intelligence- and security services, fundamental legal norms are the Act of 30 November 1998 regulating the intelligence- and security services, *BS* 18 December 1998 (as amended by the Act of 4 February 2010 concerning the methods for gathering data by intelligence- and security services, *BS* 10 March 2010) and the Royal Decree of 12 October 2010 determining the modalities of the legal obligation to cooperate in case of demands concerning electronic communications by the intelligence- and security services, *BS* 8 November 2010 (hereafter: 'Royal Decree 12 October 2010').

[14] The service providers are obliged to erase these data or make these data anonymous from the moment they are not longer necessary for the transmission of communication: art. 122, §1 AEC. However, some exceptions are possible concerning invoices (art. 122, §2), marketing (art. 122, §3) and the investigation of fraud (art. 122, §4).

[15] Response to the advice nr. 24/2008 of the Privacy Commission of 2 July 2008, Bill modifying diverse articles, *supra* note 4, consulted via http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf, lastly on 25 November 2011, 13-14 (hereafter: 'Response to advice nr. 24/2008).

of 'operators of electronic communication networks' and 'providers of electronic communication services'[16] in order to identify the user of a service of electronic communication and to identify these services of electronic communications, by a *well-founded and written* decision. The motivation of the *procureur* has to reflect the proportionality respecting the privacy and subsidiarity in relation to any other act of research. In case of an 'extremely urgent necessity', each officer of the judiciary police can, after the prior and oral consent of the *procureur*, by a well-founded and written decision, demand these data. This officer communicates this well-founded and written decision and the obtained information to the *procureur* in the following twenty-four hours and motivates the 'extremely urgent necessity'.

11. Art. 88*bis* CCP allows the *juge d'instruction* (the examining magistrate) to demand the cooperation of the service provider in order to track the localization data and origin of destination of telecommunication. He has to state the factual circumstances of the cases which justify his demand in in a well-founded warrant that he communicates to the *procureur*. The *procureur* is also competent to make a similar demand, but only in case of *flagrante delicto* and only for the punishable facts that are listed in art. 90*ter*, §§2,3 and 4 CCP. If he makes a similar demand, this demand must be confirmed within twenty-four hours by the *juge d'instruction*.

12. In the Royal Decree of 9 January 2003, an institution called the "Cell of Coordination Justice" (hereafter: 'CJ') is being installed in each service provider. This Cell consists of certain persons who are responsible for handling the demands from the judicial services concerning the data that is being retained by the service providers they work for.[17] This Decree imposes some technical obligations on the service providers, *e.g.* the obligation for the CJ to allow the NTSU-CTIF[18] to consult the client-database[19] and the obligation to "transmit [the data] in *a safe way* so the data

---

[16] The definition of 'operator' or 'provider' has been troublesome in practice: *e.g.* Yahoo! was judged not to be either an 'operator' nor 'provider' in the sense of this article. See Ghent 30 June 2010, unpublished, consulted via http://www.legalworld.be/legalworld/uploadedFiles/Rechtspraak/De_Juristenkrant/YAHOO%20Arrest%203 0%20juni%202010.pdf?LangType=2067, lastly on 25 November 2011. See for criticism P. VAN LINTHOUT, "Yahoo is geen verstrekker van elektronische communicatiedienst", *Juristenkrant* 27 October 2010, 4-5.
However, a recent arrest of the *Cour de Cassation* annulled this decision: Cass. 18 January 2011, P.10.1347.N, unpublished, consulted via http://jure.juridat.just.fgov.be, lastly on 25 November 2011.

[17] Art. 2, §1 Royal Decree 9 January 2003, *supra* note 13.

[18] National Technical & Tactical Support Unit - Central Technical Interception Facility.

[19] Art. 3, §2 Royal Decree 9 January 2003, *supra* note 13.

will not be able to be intercepted by third parties"[20] (emphasis added). The CJ will communicate the required data to the judicial services via a secured electronic pathway,[21] which has to meet specified standards.[22]

2.2.2 ACTUAL PRACTICE

13. Despite the absence of an obligation to retain specific data, service providers do retain a serious amount of data and the judicial authorities already demand these data.[23] The only possible consequence judicial authorities can face, is that previously retained data are already erased (according to the art. 122, §1 AEC).

The actual situation already allows judicial services to have access to retained data. The articles 46*bis* and 88*bis* CCP (that provide this possibility) have been applicable respectively since 24 March 2007 (46*bis*) and 10 February 1998 (88*bis*). At the current stage, judicial services have access to certain data which are not mentioned in the Directive,[24] due to the fact that service providers already retain them, even without a formal obligation to do so.

2.2.3 MEASURES TO COUNTERATTACK POSSIBLE ABUSE

14. As in any other constellation of legal norms, the risk of abuse of retained data by the judicial authorities is more than real: the articles 46*bis* and 88*bis* cannot prevent the fact that the *procureur* or the *juge d'instruction* are able to issue certain demands when the legal conditions are not met or other cases of possible abuse of these data. Thus the questions rises how this can be avoided (by preventive measures) or sanctioned (by reactive measures) according to the applicable law.

A PREVENTIVE MEASURES

a) A supervising authority

15. Confining the competence to the CJ to refuse manifestly ill-founded demands is not possible according to the applicable legal norms[25] and should not be a possibility according to me, since there is no possibility that the CJ will be aware of the exact content of the demand and the competence

[20] Art. 6, §1, 5° Royal Decree 9 January 2003, *supra* note 13.

[21] Art. 10*bis* Royal Decree 9 January 2003, *supra* note 13.

[22] Art. 6 Royal Decree 9 January 2003, *supra* note 13.

[23] Response to advice nr. 24/2008, *supra* note 15, 27.

[24] These data concern (identification of) the user of the services: Response to advice nr. 24/2008, *supra* note 15, 27.

[25] Art. 46*bis*, §2, al. 4 and 88*bis*, §2, al. 3 CCP explicitly provide a penal sanction for refusal of cooperation.

to refuse ill-founded demands can better be confined to an impartial judge. The *juge d'instruction* fulfills this requirement, but it can hardly be argued that the *procureur* has a comparable level of impartiality.

b) A 'safe way' to access the data

16. According to art. 6, §1, 5° Royal Decree 9 January 2003, the service providers must ensure a safe way for the transmission of data. Art. 2, §6 of the same Decree obliges service providers to take all necessary measures in order to guaranty the confidentiality of the information that is being used by the CJ. In this way, third parties that do not have to competence to require the stored data should not be able to obtain them.

B REACTIVE MEASURES

c) Supervising authorities

17. The Belgian Institute for the Post- and Telecommunication Sector (BIPT) is competent to control the respect for the AEC and its executing Decrees.[26] The BIPT has the competence to issue administrative fines, which can be up to 5% of the turnover (with a maximum of €12.500.000).[27] Except this institute, the Privacy Commission, the manager of the CJ and judicial services can also be mentioned as supervision authorities relative to the application of legal norms concerning data retention.[28]

d) Incriminations

i)Art. 39 Privacy Act

18. According to art. 39 Privacy Act, persons that breach art. 4 of the same act (*e.g.* by incompatible use of the data, storage of too many data…) can be given a fine between €100 and €100.000. As well as the control of the supervising authorities, this control mechanism is only indirectly useful for data retention.

ii)Art. 210bis, 458, 504quater, 550bis, §§1-2 of the Criminal Code.

19. These articles of the Criminal Code are phrased in a very general way and do not provide in a specific sanction for the breach of duties concerning data retention. Notwithstanding their general scope, they can still be very useful: *e.g.* art. 550*bis*, §§1-2 (which concerns internal and external hacking)

[26] Art. 14, 3° of the Act of 17 January 2003 concerning the statute of the regulator of the Belgian post- and telecommunication sectors, *BS* 24 January 2003.

[27] Art. 21 of the same Act.

[28] Bill modifying diverse articles, *supra* note 4, 17, nr. 6.

is applicable when unauthorized persons have had access to the data (§1) or when authorized persons have had access, but have exceeded their legal competence (§2). The other articles refer to fraud involving informatics (art. 210*bis* and 504*quater*) and the violation of professional secrecy[29] (art. 458).

e) Possibility for service providers to complain

20. Demands from the judicial services are being dealt with by the NTSU-CTIF unit of the federal police. This unit needs to have access to the client database of the service providers that have a 'numberingcapacity'.[30] Service providers can see when this unit has had unauthorized access and have the possibility to address this issue.[31] Since they have to give an automated response to the requests made by the NTSU-CTIF unit,[32] there is no possibility to refuse ill-founded demands.

2.2.4 CRITICAL APPROACH

A IN GENERAL

21. Generally speaking, the current Belgian approach regarding judicial services does not seem to be a justified interference with the right of privacy. In order for an interference to be justified, it has to be (1) provided by law, (2) striving for a legitimate aim and (3) necessary in a democratic society.

The first and second condition do not seem to pose insurmountable problems concerning the Belgian situation[33], but the third is problematic.

22. A first issue concerning the question of necessity is whether the imposed measures are adequate to achieve their goal. In my opinion, certainly organized crime will be able to circumvent most, if not all, imposed measures: they will *e.g.* know how to hide their IP-addresses or make it impossible to trace their calls. According to me, this does not automatically imply that data retention is not necessary, since the circumvention of these measures requires some technical skills and not

[29] Art. 46*bis*, §2, al. 3 and art. 88*bis*, §2, al. 2 impose a duty of secrecy to everybody who, in the execution of their function, comes in to contact with these data or cooperates in this procedure.

[30] Art. 3, §2 Royal Decree 9 January 2003, *supra* note 13.

[31] Commission for the Protection of Privacy, Advice concerning the Bill and the Draft of Royal Decree relative to data retention, and the Draft of Royal Decree relative to the obligation to cooperate (A/09/012), 1 July 2009, nr. 20/2009, consulted via http://www.privacycommission.be/nl/docs/Commission/2009/advies_20_2009.pdf, lastly on 25 November 2011 (hereafter: 'Advice nr. 20/2009'), 14, nr. 43.

[32] Art. 3, §2 Royal Decree 9 January 2003, *supra* note 13.

[33] See however concerning the Data Retention Directive, Opinion EDPS 2011, *supra* note 2, 12-14, nrs. 64-73 in which the Directive is being judged as not meeting the requirement of foreseeability.

everybody that commits a 'serious crime' will possess that ability.

Apart from this point, conclusions can only be drawn very reticently from the gathered data and a cautious approach should be taken. How can we be sure that the person who is calling to X is really the person that is identified by the service provider etc.? The adequacy of the applicable norms can never be completely assured, but the usage of more data can offer a larger probability. In all, the issue of adequacy remains troublesome.

23. Regarding necessity in general, the legislator has tried to adopt measures that do not go further than necessary.[34] Nonetheless, some doubts raise whether no less intrusive techniques could have been used and whether the right of privacy is in no way more infringed than absolutely necessary. In all, this attempt to balance combined with the following remarks do not make the actual interference justified in my opinion.

B REGARDING THE LEGAL NORMS THAT ALLOW ACCESS (ART. 46BIS AND 88BIS CCP)

24. The possibility for the *procureur* to demand retained data is quite limited, and therefore held proportional[35]: if the *procureur* wants to know to whom a certain phone number belongs, he can make a similar demand according to art. 46*bis*, but if he needs information concerning the persons who have been called from this number, the *juge d'instruction* has to make the demand according to art. 88*bis*.[36] The organizational arguments and the restricted competence for the *procureur* (*i.e.* that the intervention of the *juge d'instruction* is required whenever a more invasive demand than the mere identification of a phone number is made) seem to be elements that provide a reasonable balance.

25. However, not every detail in these articles seems to be as proportionate. An element that seems disproportional to me is the possibility that the consent of the *procureur* has to be only oral in case of an 'extremely urgent necessity': in modern times, requiring a written consent in each situation does not seem impracticable to me.[37] But it is the absence of a clear and effective sanction for abuses of this possibility that really

[34] See concerning art. 46*bis* and art. 88*bis* Exposure of Motives of Government bill 12 June 1997 modifying the Act of 30 June 1994 concerning the protection of privacy against eavesdropping, taking note and registration of private communications and telecommunications, *Parl.St.* Senate 1996-97, nr. 1075/1, 1-7.

[35] Exposure of Motifs of the Project of Act modifying article 46*bis* of the Code of Criminal Procedure, *Parl.St.* Senate 2005-06, nr. 3-1824/1, 5.

[36] Report 8 December 2006 in the name of the Commission of Justice by W. Muls of the Government bill modifying article 46*bis* of the Code of Criminal Procedure, *Parl.St*. Chamber 2006-07, nr. 51-2724/2, 6 (hereafter: 'Report Muls').

[37] A similar remarks has been made by S. VERHERSTRAETEN: see Report Muls, *supra* note 36, 6.

makes these articles disproportional to me.

26. The competence of the *procureur* to make these demands whenever he deals with '*délits*' or *crimes* and the competence of the *juge d'instruction* to make these demands whenever he *'judges that there are circumstances that make a detection of telecommunications or a location of the origin or destination of telecommunications necessary to unveil the truth'*[38] seem to be other problems.

27. The wide scopes of these articles will encompass a very large amount of incriminated behavior, and the question rises whether such a broad scope is justified. The Privacy Commission made the remark (concerning art. 46*bis* CCP) that this scope is too wide and that an exhaustive list of offences is to be preferred, by analogy of art. 90*ter* CCP concerning the tapping of private communication.[39] The legislator disagreed, stating that it is not doable to make such a list, that guaranties concerning subsidiarity and proportionality are already present and that the addition of new offences to the list would be too time-consuming and difficult,[40] so the very general description of '*délits* and crimes' has been maintained in art. 46*bis* CCP. Recently, the European Commission stated that "[m]ost transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes, *going beyond those covered by the Directive, including preventing and combating crime generally*"[41] (emphasis added), thereby implying that 'serious crime' is more limited than the transposition of –at least some– Member States.

28. In my opinion, there is no apparent necessity for the legislator to encompass such a broad specter of offences: the Directive mentioned 'serious crime' and it seems to me that (1) not every offence that falls under the scope of the mentioned articles is necessarily a 'serious crime'[42] and that (2) the importance of privacy prohibits such a more extensive interpretation of this term in national legislation. Moreover, the possibility is available to make this required exhaustive list: art. 90*ter* CCP already foresees in such a list, so why would this be impossible in relation to data retention? According to me, lists of specific offences in both art. 46*bis* and art. 88*bis* CCP are essential elements in order to justify the serious interference with the right of privacy.

38 Art. 88*bis*, §1, al. 1 CCP.

39 Advice nr. 24/2008, *supra* note 12, 10-11, nrs. 25-26.

40 Bill modifying diverse articles, *supra* note 4, 14-15, nr. 5.

41 Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 Final, 8 (hereafter: 'Evaluation Report'); Opinion EDPS 2011, *supra* note 2, 13, nr. 72.

42 In my opinion, art. 46*bis* and 88*bis* CCP are used for 'preventing and combating crime generally'.

C REGARDING THE MEASURES TO COUNTERATTACK POSSIBLE ABUSES

f) Supplementary incrimination

29. In order to comply with art. 13(2) of the Directive, a supplementary and specific incrimination concerning abuse of retained data seems necessary. The legislator shared this opinion in the Bill modifying diverse articles,[43] but since the Bill did not get adopted, a supplementary incrimination is yet to be issued.

g) Sanction for the usage of irregularly obtained data?

30. Since the usage of irregularly obtained proof in criminal cases is being subjected to the so-called 'Antigoon' doctrine (which does not exclude *ipso facto* the usage of these data) and privacy is severely compromised by the usage of retained data, a nullity sanction of the irregularly obtained data seems more than necessary.[44] The argument of the legislator that it would 'not [be] logic' to foresee in such a sanction in this Act[45] is not compelling: the link between data retention and sanctions for irregularly obtained data is inherent to any norm regarding data retention, so that these sanctions can (and should) be provided by these norms.

h) 'Safe access'

31. Some questions can arise concerning the obligations for service providers to ensure the safe transmission of data.[46] Is this the best way to ensure the safety of the data? I think there should be at least a thorough test to check whether the specific way of transmitting data is really secure, since –at this stage- the safety of the data is not properly ensured in my opinion.[47]

2.2.5 CONCLUSION CONCERNING THE JUDICIAL SERVICES

32. The adequacy of the usage of retained data seems to be a fundamental problem which can never be completely solved. The only way to cope with

---

43 *Supra* note 4.

44 In the same sense: Order of Flemish Bar Councils, *Standpunt – Een kritische reflectie van de Europese databewaringsrichtlijn*, consulted via http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/20091026_Standpunt_Orde_van_Vlaamse_Balies.pdf, lastly on 25 November 2011, 2.

45 Bill modifying diverse articles, *supra* note 4, 17, nr. 7.

46 See *supra* nr. 16.

47 See concerning general measures relative to the protection of processed data, Commission for the Protection of Privacy, "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens", consulted via http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf, lastly on 25 November 2011.

this problematic issue is to refrain from reversing the presumption of innocence and to adopt a very cautious attitude towards drawing conclusions from the gathered 'evidence'.

33. Although the legislator has tried to strike a reasonable balance between security issues and the right of privacy, the following elements still make the interference with the right of privacy unjustified:

- the consent of the *procureur* has to be only oral in case of an 'extremely urgent necessity';
- a supplementary and specific incrimination concerning abuse of retained data is absent;
- a nullity sanction for irregularly obtained data is absent;
- the scope of art. 46*bis* and 88*bis* CCP is too wide;
- the safety of the data transmission is only to be dealt with by the service providers.

34. The common denominator in the first three remarks is the absence of an adequate and specific mechanism that supervises every element in the procedure of gaining access to the retained data (and that sanctions adequately every abuse); the last two problems can only be solved by specific measures.

2.3 INTELLIGENCE - AND SECURITY SERVICES

2.3.1 SPECIFIC LEGAL NORMS

35. As mentioned above,[48] the Act of 30 November 1998 regulating intelligence- and security services[49] and the Royal Decree of 12 October 2010 determining the modalities of the legal obligation to cooperate in case of demands concerning electronic communications by the intelligence- and security services[50] form the fundamental norms regarding the possibility for intelligence- and security services. The Royal Decree of 12 October 2010 is almost identical to the amended Royal Decree of 9 January 2003[51], with the consequence that no further comment on this Decree will be made[52], except for the obligation to preserve information concerning the identity of the

48 *Supra*, note 13.

49 *Ibid*.

50 *BS* 8 November 2010. This Decree implements art. 18/7, 18/8, 18/17 and 18/18 of the previously mentioned law and art. 127, §1, al. 1, 2° AEC.

51 S*upra*, note 13.

52 See *supra* nrs. 12, 16 and 20 for comments on the (amended) Royal Decree of 9 January 2003, *supra* note 13.

person that makes the demand for ten years.[53] This obligation will provide a better way to remark and investigate possible abuses.[54]

36. The articles 18/7 and 18/8 Act 30 November 1998 are the respective counterparts of the articles 46*bis* and 88*bis* CCP. The content of these dispositions are identical, except for the subjects that are competent to demand certain retained data: where in art. 46*bis* the *procureur* and in art. 88*bis* the *juge d'instruction* have this competence, the head of service has it according to art. 18/7 and 18/8.

37. In the preparatory works of this Act, the necessity to balance the fundamental rights of individuals and the security of the State is one of the first topics mentioned.[55] The professional secret needs to be treated with a specific protection, having regard to its specific importance.[56] Also, the specificity of the intelligence- and security services are emphasized: these services are (to a certain extent) not comparable to the judicial services, since the former aim at an intellectual investigation of networks that can pose a threat to society, while the latter focus on the gathering of proof concerning offences.[57]

2.3.2 MEASURES TO COUNTERATTACK POSSIBLE ABUSE

A ABSENCE OF PREVENTIVE MEASURES

38. No preventive measures are available to control possible abuses: the supervising authorities will only have an *a posteriori* control. The legislator held this to be justified: a certain flexibility in the operations of the intelligence- and security services is deemed to be necessary, since a too demanding procedure would impede these services to work properly.[58]

B REACTIVE MEASURES

i) The administrative commission

39. According to art. 43/1 Act 30 November 1998, an administrative

53 Art. 3, §2, al. 3 Royal Decree 12 October 2010, *supra* note 13.

54 Commission for the Protection of Privacy, Advice relative to the Draft of Royal Decree determining the modalities of the legal obligation to cooperate in case of demands concerning electronic communications by the intelligence- and security services, 30 June 2010, nr. 23/2010, consulted via

http://www.privacycommission.be/nl/docs/Commission/2010/advies_23_2010.pdf, lastly on 25 November 2011, 3, nr. 9.

55 Private Member's bill 10 December 2008 concerning the methods for the collection data by the intelligence- and security services, *Parl.St.* Senate 2008-09, nr. 4-1053/1, 1 (hereafter: 'Private Member's bill 10 December 2008').

56 *Ibid.*, 14-17.

57 *Ibid.*, 12.

58 Private Member's bill 10 December 2008, *supra* note 55, 26.

commission is established in order to supervise the specific and exceptional methods for the gathering of data by intelligence- and security services. Among the specific methods, the demands of retained data are specified and mentioned,[59] with the consequence that this commission controls the gathering of these data as well.

The commission has different competences depending on the type of measure concerned: the commission will only have an *a posteriori* control with it comes to these specific methods.[60] At the end of each month, each service has to send detailed lists of the used specific methods, so that the commission could properly control the usage of these methods.[61]

j) The Fixed Comity I[62]

40. According to art. 43/2 Act 30 November 1998, the Fixed Comity I is obliged to control *a posteriori* the same specific and exceptional methods (and thus the relevant demands of retained data as well). This Fixed Comity I has, *inter alia*, the competence to judge the legality of the used methods, as well as the respect of the principles of proportionality and subsidiarity.[63] It cannot only act *motu proprio*, but also (*inter alia*) on the request of the Privacy Commission or on the basis of a complaint.[64]

When this Comity concludes that the used method was illegal, the method has to be terminated and the acquired data must not be exploited and have to be destroyed.[65]

2.3.3 CRITICAL APPROACH

41. Does the criticism of the approach concerning the judicial services apply to these norms as well? Regarding the problematic issues of that approach[66], the first four are not as troublesome.

42. According to art. 18/7, §2 Act 30 November 1998, the officer of the intelligence service can request orally the concerned data in case of an 'extremely urgent motivated necessity', provided that he has the prior oral

---

59 In art. 18/2, §1, 4°, the gathering of identification data of users of electronic communication is mentioned and in art. 18/2, §1, 5°, the research of call data and localization of origin or destination of electronic communication is notified.

60 Private Member's bill 10 December 2008, *supra* note 55, 26. Concerning *exceptional* methods, it will have to give its prior consent.

61 *Ibid.*

62 The Fixed Comity on the Supervision of Intelligence Services.

63 Art. 43/2, al. 2 Act 30 November 1998, *supra* note 13.

64 Art. 43/4, 1st-3rd bar Act 30 November 1998, *supra* note 13.

65 Art. 43/6, §1, al. 1. Act 30 November 1998, *supra* note 13.

66 See *supra* nr. 33.

consent of the head of service. The head of service will confirm as soon as possible this oral consent by a written and motivated decision. Contrary to the situation of the judicial services, a specific authority supervises every decision in relation to specific methods. By installing this specific administrative commission, a fair balance has been struck in this situation according to me.

43. The second (concerning a supplementary incrimination) and third remark (concerning the nullity sanction for irregularly obtained data) are not applicable either, due to the presence of the same commission. The supplementary incrimination and the nullity sanction for irregularly obtained data are deemed necessary in the situation of the judicial services because of the absence of adequate control mechanisms; since a specific and adequate administrative commission is present, these two problems seem to be solved as well.

44. The fourth remark, regarding the scope of art. 46*bis* and 88*bis* CCP, does not apply here. The competence of the head of service to make requests concerning retained data 'whenever this is of importance for the execution of the missions'[67] can be justified by referring to the specific mission of the intelligence- and security services.

45. The only remark that is also applicable on the access of intelligence- and security services is the last one (regarding the safety of the data transmission). According to art. 8, §1, 5° Royal Decree 12 October 2010, the service provider must ensure a safe way for the transmission of data. Again, a specific test to check whether the specific way of transmitting data is really secure seems to be necessary.

2.3.4 CONCLUSION CONCERNING THE INTELLIGENCE- AND SECURITY SERVICES

46. Contrary to the legal norms governing the judicial services, the norms that are applicable to the intelligence- and security services seem rather proportionate to me, provided that the same cautious approach is taken whenever conclusions are drawn from the gathered data.

Apart from the omnipresent issue of adequacy, a supplementary safety-check of the way providers transmit data seems to be to only issue.

2.4 CONCLUSION CONCERNING THE BELGIAN APPROACH *DE LEGA LATA*

47. The actual situation in Belgium concerning data retention is fragmented

[67] Art. 18/7, §1 and 18/8, §1 Act 30 November 1998, *supra* note 13.

and complex, since no general and systematic implementation of the Data Retention Directive has been issued.

Notwithstanding the absence of any obligation for service providers to retain certain data, the actual practice is that judicial-, intelligence- and security services demand the necessary data from these providers. Due to the absence of such an obligation, these services will sometimes be confronted with the fact that the requested data have been erased according to the Act on Electronic Communication.

48. In my opinion, the present situation concerning judicial services does not provide the required guarantees in order to achieve the necessary balance between the need for judicial services to use this data and the right of privacy. An independent authority should be installed in order to deal with possible problems concerning the oral consent of the *procureur*, the absence of a specific incrimination and the absence of a nullity sanction for irregularly obtained data; the scope of the relevant articles should be narrowed, a limitative list of 'serious crimes' should be established and a thorough test should be provided to check whether the data transmission mechanisms used by the service providers are sufficient.

49. On the contrary, the situation concerning intelligence- and security services offers guarantees to deal with possible abuses in an effective way so that it seems rather proportionate (except maybe for the data transmission mechanisms).

50. The most problematic point concerning the present situation is that the above-mentioned services have far greater competences when it comes to access of retained data than is being realized. At this moment, only other (even more) invasive measures are not getting agreed upon following the parliamentary procedure.[68] However, at this moment, numerous types of data are being retained by the providers[69] and are accessible for these services, with the consequence that the disperse and unclear regulation of data retention in Belgium is more privacy-invasive than it appears to be on first sight.

3. THE BELGIAN APPROACH *DE LEGE FERENDA*

51. In this chapter, the Bill modifying diverse articles and the Draft of Royal Decree[70] will be examined, since the legislator tried to transpose the Directive by using these two instruments.

---

68 See *infra* nrs. 51-58.

69 See Response to advice nr. 24/2008, *supra* note 15, 27.

70 See *supra* note 8 for their complete titles.

Firstly, the goal of these legal norms will be examined (3.1); secondly, an analysis will be made of the data that are to be retained according to the Royal Decree (3.2). Thirdly, the duration of the obligation to retain will be dealt with (3.3). Fourthly, the supplementary measures to cope with possible abuses are being discussed (3.4). Fifthly, an general evaluation will be made of these propositions (3.5). Finally, an overall view of the future of data retention in Belgium will be made (3.6).

3.1 THE GOAL OF THE PROPOSITIONS

52. The goal of the above-mentioned norms is wider than the research, prosecution and repression of criminal infractions (which constitute serious criminality). Repression of malicious calls to emergency services and research by the Mediation service for telecommunication of the identity of persons having made malicious use of an electronic communication network or service are other goals,[71] but the repression of serious criminality remains the most important one. The Privacy Commission has (correctly) made some critical remarks concerning these other two goals: since their access to retained data is based on other purposes than the investigation of criminal infractions, other conditions for their access should be required and even better would be that their access is dealt with in separate legislation.[72]

3.2 WHAT DATA ARE TO BE RETAINED?

53. According to the Draft of Royal Decree, the data listed in the Directive do not suffice,[73] since the necessities of the police services require a more extensive list.[74]

The justification of the supplementary identification data is that (1) it is necessary for the identification of users of communication services and (2) these data only relate to the user and not to the traffic data (and are therefore proportional).[75]

Except these identification data, some traffic data are also concerned:

- personal data (delivery- and invoice addresses);
- payment data (type of payment, identification of the mean of payment, data and time of payment);

71 Art. 3, §1, al. 3 Bill modifying diverse articles, *supra* note 4, 34-35.

72 Advice nr. 24/2008, *supra* note 12, 13, nr. 30.

73 Report to the King of the Draft of Royal Decree, *supra* note 8, http://stefaandecler-ck.be/files/pdf/ dataretentie_KB.pdf, lastly on 25 November 2011, 1.

74 Response to advice nr. 24/2008, *supra* note 15, 25-26.

75 *Ibid.*, 26-27.

- technical data relative to the creation of an account on an internet service (IP-address, network connection point);
- information concerning the transfer of a phone number.[76]

54. Questions arise concerning the necessity to extend the list of data provided by the Directive. The usefulness of these supplementary data is clear, but does it outweigh the supplementary infringement of the right of privacy? In my opinion, a detailed and specific impact assessment is not doable in this case, so that the given justifications of this extension can appear reasonable, provided that an evaluation of the necessity of these supplementary data will take place not long after these legal norms are in force.[77] According to the Bill modifying diverse articles, such an evaluation will take place two years after the Royal Decree would have come in force.[78]

3.3 HOW LONG MUST THE DATA BE RETAINED?

55. Originally, the legislator intended to insert a duration of 24 months.[79] After critical remarks from the Privacy Commission[80], the legislator reduced the duration to 12 months, with an exception for exceptional circumstances which can justify a duration longer than 12 months.[81] If the duration would exceed 24 months, the other Member States and the European Commission will be informed. If the Commission does not decide within a period of six months after the notification, the prolongation will be deemed approved.[82]

56. In the actual situation, these durations seem too long. According to information from the federal judicial police of 2007,[83] only 15% of all requests relate to data less than six months old, 51% relates to data between six and twelve months old and 34% is older than twelve months. However, these data seem to be somewhat contradicted by the Evaluation Report of the European Commission. This report shows that 86% of all requests relate to data less than six months old, 12% relate to data between six and twelve months old and only 2% relate to data that are older than one year.[84]

At this stage, a thorough reevaluation of the appropriate duration has to take place before continuing the parliamentary procedure concerning the

76 *Ibid.*, 28-30. For each of these traffic data, a specific justification is listed.
77 In the same sense: Advice nr. 20/2009, *supra* note 31, 14, nr. 14.
78 Art. 3, §4 of the Bill modifying diverse articles, *supra* note 4, 36.
79 Advice nr. 24/2008, *supra* note 12, 13, nr. 33.
80 *Ibid.*, 13-15, nrs. 33-36.
81 Art. 3, §1, al. 4 and §2, al. 1 of the Bill modifying diverse articles, *supra* note 4, 35.
82 Art. 3, §2, al. 2-3 of the Bill modifying diverse articles, *supra* note 4, 35-36.
83 Response to advice nr. 24/2008, *supra* note 15, 32.

Draft of Royal Decree.

3.4 WHAT SUPPLEMENTARY MEASURES TO COPE WITH ABUSES ARE PROVIDED?

57. After having read the remarks of the Privacy Commission that a supplementary incrimination should be provided,[85] the legislator adapted his Bill modifying diverse article in order to install this extra incrimination.[86] Apart from this (useful and necessary) extra incrimination, no further measures are taken by the Bill and the Draft Royal Decree.

58. Still, a specific authority should supervise every usage or decision in relation to usage of retained data. The BIPT[87] and the Privacy Commission are useful supervising authorities, but they are not sufficient to counterbalance the possible abuse of oral consents of the *procureur* nor the absence of a nullity sanction for irregularly obtained data.

3.5 GENERAL EVALUATION OF THE PROPOSITIONS

3.5.1 THE CHOICE FOR A ROYAL DECREE

59. There has been quite a discussion about the use of a Royal Decree to transpose some very essential norms: the legislator argued that a Royal Decree is (1) necessary for a 'quick update' and is (2) not contrary to the will of the legislator;[88] the Order of Flemish Bar Councils emphasizes the fact that the usage of a Royal Decree is 'unacceptable' since crucial elements will not be subjected to a 'thorough and ample parliamentary debate';[89] the Privacy Commission found the choice for a Royal Decree 'difficult to reconcile' with choices made in the Directive.[90] In my opinion, the usage of a Royal Decree should be avoided: for me, the necessity for a 'quick update' does not outweigh the need for an (at least possibly) thorough debate.

---

84 Report Comm. 18 April 2011 from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 Final, 22. Since the goal of the Directive is to harmonize the national legislations (art. 1 Directive), a period of six months seems more appropriate if, after a serious impact assessment, the legislator is of the opinion that the Directive should still be transposed.

85 Advice nr. 24/2008, *supra* note 12, 23, nr. 65.

86 Art. 4 of the Bill modifying diverse articles, *supra* note 4, 37.

87 See *supra* nr. 17.

88 Exposure of Motives of the Bill modifying diverse articles, *supra* note 4, consulted via http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf, 4 and Response to advice nr. 24/2008, *supra* note 15, 19.

89 Order of Flemish Bar Councils, *Standpunt – Een kritische reflectie van de Europese databewaringsrichtlijn*, consulted via http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/20091026_Standpunt_Orde_van_Vlaamse_Balies.pdf, 2.

90 Advice nr. 24/2008, *supra* note 12, 13, nr. 32.

3.5.2 NECESSITY OF PROPOSITIONS IS NOT DEMONSTRATED

60. The issue of necessity has not been sufficiently dealt with in the underlying prepositions. Firstly, the above-mentioned[91] issues concerning the adequacy reappear and secondly, no demonstration of the necessity of these propositions has been made.

At first, the propositions were not conclusive concerning their own necessity;[92] afterwards, the Privacy Commission correctly raised the question why the existing norms do not suffice.[93] The response of the legislator[94] was, in my opinion, completely insufficient, due to the following three factors:

- no *quantitative* nor *qualitative* statistical information has been used, although the actual practice concerning the existing norms (46*bis* and 88*bis* CCP) could provide the required data to make an impact assessment;
- no reference to the possibility of data preservation[95] has been made, nor has it been considered as an (at least partial) alternative for data retention: the only alternative considered was the interception of the content of electronic communication;
- no balance between the right of privacy and the usefulness of these data for the authorities has been made: only the fact that some crimes cannot be solved without data retention was mentioned.[96]

3.6 CONCLUSION CONCERNING THE FUTURE OF DATA RETENTION IN BELGIUM

61. At this moment, the deadline foreseen for the approval of both the Bill modifying diverse articles and the Draft Royal Decree has not been met "due to the collapse of the government".[97] In general, the resistance of civil society organizations has proved to be efficient to prevent the Bill and Draft Royal Decree of coming in force, but maybe even more important is the situation on the European level.

[91] See *supra*, nr. 22.

[92] Advice nr. 24/2008, *supra* note 12, 7, nr. 16.

[93] *Ibid.*

[94] Response to advice nr. 24/2008, *supra* note 15, 10.

[95] Of course, data preservation will not help to solve every crime, but at least a thorough analysis of its use should have been made. In the same sense (concerning the Directive): Opinion EDPS 2011, *supra* note 2, 10-11, nrs. 53-57.

[96] Response to advice nr. 24/2008, *supra* note 15, 10-11.

[97] Statement made on the website of Minister of Justice, Stefaan De Clerck: http://www.stefaandeclerck.be/nl/dataretentie/941.

In its report, the Commission acknowledges that the current approach of data retention needs to be revised.[98] In order to do so, the Commission will execute an impact assessment, so that further practical evidence can be gathered in order to demonstrate the necessity of European measures concerning data retention.[99] This impact assessment should also examine whether other, less privacy-intrusive measures can be appropriate,[100] but as a consequence the future of data retention on a European level is uncertain: it may well be the conclusion of the impact assessment that other, less intrusive means than data retention can be used to achieve the same goal.

62. In this European perspective, the future of data retention in Belgium seems highly uncertain as well. If the resistance from civil society organizations already prevented a complete and full transposition of the Directive, chances are minimal that the above-mentioned Bill and Draft Royal Decree will be approved having regard to the current insecure future of the European approach.

4. GENERAL CONCLUSION

63. Seeing the chances of having a complete transposition being minimized does however not imply that an imminent danger has been avoided: in the second chapter, it has been argued that the actual situation of data retention in Belgium is more privacy-intrusive than it appears to be on first sight.[101]

64. The absence of any future measures will have the negative effect that a thorough and broad assessment of the actual situation will probably not be a political priority. Nonetheless, it has been argued that the applicable legal norms regarding the judicial services should be seriously revised, since the Belgian approach at this moment does not seem to meet the requirements concerning data protection and privacy.[102]

65. In all, as for the European level,[103] all possibilities should be considered and a serious and ample debate about data retention in Belgium should be a political priority, having regard to the severe infringement of the right of privacy, even by the norms that are currently applicable.

REFERENCES

98 Evaluation Report, *supra* note 41, 32-33.
99 *Ibid.*, 30.
100 Opinion EDPS 2011, *supra* note 2, 14, nr. 76.
101 See *supra*, nr. 50.
102 See *supra*, nrs. 33 and 48.
103 See Opinion EDPS, *supra* note 2, 14-15, nrs. 74-82.

Legislation

European Legislation

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L281, 23 November 1995, 31.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L28*1*, 23 November 199*5*, 3*1*.

[3] 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, *OJ* L201, 31 July 2002, 37 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, *OJ* L337, 18 December 2009, 11.

[4] 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* L105, 13 April 2006, 54 (also referred to as 'the Data Retention Directive').

Belgian Legislation

[1] Act of 21 March 1991 concerning the reform of certain economic public enterprises, *BS* 27 March 1993.

[2] Act of 21 March 1991 concerning the reform of certain economic public enterprises, *BS* 27 March 1993.

[3] Act of 8 December 1992 relative to the protection of privacy with regard to the processing of personal data, *BS* 13 March 1993 (also referred to as 'Privacy Act')

[4] .Act of 30 November 1998 regulating the intelligence- and security services, *BS* 18 December 1998 (as amended by the Act of 4 February 2010 concerning the methods for gathering data by intelligence- and security services, *BS* 10 March 2010) (also referred to as 'Act 30 November 1998').

[5] Act of 17 January 2003 concerning the statute of the regulator of the Belgian post- and telecommunication sectors, *BS* 24 January 2003.

[6] Act of 13 June 2005 concerning electronic communication, *BS* 20 May 2005 (also referred to as 'AEC').

[7] Code of Criminal Procedure.

[8] Royal Decree of 13 February 2001 executing the Act of 8 December 1992 relative to the protection of privacy with regard to the processing of personal data, *BS* 13 March 2001.

[9] Royal Decree of 9 January 2003 determining the modalities of the legal obligation to cooperate in case of judicial demands concerning electronic communications, *BS* 10 February 2003, as amended by the Royal Decree of 8 February 2011, *BS* 10 February 2011 (also referred to as 'Royal Decree 9 January 2003').

[10] Royal Decree of 12 October 2010 determining the modalities of the legal obligation to cooperate in case of demands concerning electronic communications by the intelligence- and security services, *BS* 8 November 2010 (also referred to as 'Royal Decree 12 October 2010').

Documents relative to legislation

Documents relative to European legislation

[1] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, consulted via www.edps.europa.eu, lastly on 25 November 2011 (also referred to as 'Opinion EDPS 2011').

[2] Report Comm. 18 April 2011 from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 Final (also referred to as 'Evaluation Report').

Documents relative to Belgian legislation

Preparatory documents

[1] Bill modifying the articles 2, 126 and 145 of the Act of 13 June 2005 relative to electronic communications and the article 90*decies* of the Code of Criminal Procedure, version of 27 August 2009, consulted via http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf, lastly on 25 November 2011 (also referred to as 'Bill modifying diverse articles').

[2] Bill modifying the articles 2, 126 and 145 of the Act of 13 June 2005 relative to electronic communications and the article 90*decies* of the Code of Criminal Procedure, version of 27 August 2009, consulted via http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf, lastly on 25 November 2011 (also referred to as 'Bill modifying diverse articles').

[3] Draft of Royal Decree establishing the data to be stored in application of the article 126 of the Act of 13 June 2005, and the conditions and the duration of the storage of these data, version of 14 August 2009, consulted via http://stefaandeclerck.be/files/pdf/dataretentie_KB.pdf, lastly on 25 November 2011 (also referred to as 'Draft of Royal Decree').

[4] Exposure of Motives of Government bill 12 June 1997 modifying the Act of 30 June 1994 concerning the protection of privacy against eavesdropping, taking note and registration of private communications and telecommunications, *Parl.St.* Senate 1996-97, nr. 1075/1.

[5] Exposure of Motifs of the Project of Act modifying article 46*bis* of the Code of Criminal Procedure, *Parl.St.* Senate 2005-06, nr. 3-1824/1.

[6] Exposure of Motives of the Bill modifying the articles 2, 126 and 145 of the Act of 13 June 2005 relative to electronic communications and the article 90*decies* of the Code of Criminal Procedure, version of 27 August 2009, consulted via http://stefaandeclerck.be/files/pdf/wet_dataretentie.pdf, lastly on 25 November 2011, 1-5.

[7] Private Member's bill 10 December 2008 concerning the methods for the collection data by the intelligence- and security services, *Parl.St.* Senate 2008-09, nr. 4-1053/1 (also referred to as 'Private Member's bill 10 December 2008').

[8] Report 8 December 2006 in the name of the Commission of Justice by W. Muls of the Government bill modifying article 46*bis* of the Code of Criminal Procedure, *Parl.St*. Chamber 2006-07, nr. 51-2724/2 (also referred to as 'Report Muls').

[9] Report to the King of the Draft of Royal Decree establishing the data to be stored in application of the article 126 of the Act of 13 June 2005, and the conditions and the duration of the storage of these data, version of 14 August 2009, consulted via http://stefaandeclerck.be/files/pdf/dataretentie_KB.pdf, lastly on 25 November 2011.

[10] Response to the advice nr. 24/2008 of the Privacy Commission of 2 July 2008, annex to the Bill modifying the articles 2, 126 and 145 of the Act of 13 June 2005 relative to electronic communications and the article 90*decies* of the Code of Criminal Procedure, version of 27 August 2009, consulted via http://stefaandeclerck.be/files/pdf/wet_data retentie.pdf, lastly on 25 November 2011, 10-33 (also referred to as 'Response to advice nr. 24/2008').

Advices

[1] Commission for the Protection of Privacy, Advice concerning the Bill modifying art. 126 of the Act of 13 June 2005 relative to the electronic communication, and concerning the Draft of Royal Decree Draft establishing the data to be stored in application of the article 126 of the Act of 13 June 2005, and the conditions and the duration of the storage of these data (A/08/024), 2 July 2008, nr. 24/2008, consulted via http://www.privacycommission.be/nl/docs/Commission/2008/advies_24_2008.pdf, lastly on 25 November 2011 (also referred to as 'Advice nr. 24/2008).

[2] Commission for the Protection of Privacy, Advice concerning the Bill modifying art. 126 of the Act of 13 June 2005 relative to the electronic communication, and concerning the Draft of Royal Decree Draft establishing the data to be stored in application of the article 126 of the Act of 13 June 2005, and the conditions and the duration of the storage of these data (A/08/024), 2 July 2008, nr. 24/2008, consulted via http://www.privacycommission.be/nl/docs/Commission/2008/advies_24_2008.pdf, lastly on 25 November 2011 (also referred to as 'Advice nr. 24/2008).

[3] Commission for the Protection of Privacy, Advice concerning the Bill and the Draft Royal Decree relative to data retention, and the Draft Royal Decree relative to the obligation to cooperate (A/09/012), 1 July 2009, nr. 20/2009, consulted via http://www.privacycommission.be/nl/docs/ Commission/2009/advies_20_2009.pdf, lastly on 25 November 2011 (also referred to as 'Advice nr. 20/2009').

[4] Commission for the Protection of Privacy, Advice relative to the Draft Royal Decree determining the modalities of the legal obligation to cooperate in case of demands concerning electronic communications by the intelligence- and security services, 30 June 2010, nr. 23/2010, consulted via http://www.privacycommission.be/nl/docs/Commission/2010/advies_23_2010.pdf, lastly on 25 November 2011.

[5] Commission for the Protection of Privacy, "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens", consulted via http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf, lastly on 25 November 2011.

Court Decisions

[1] Cass. 18 January 2011, P.10.1347.N, unpublished, consulted via http://jure.juridat.just.fgov.be, lastly on 25 November 2011.

[2] Ghent 30 June 2010, unpublished, consulted via http://www.legalworld.be/legalworld/uploadedFiles/Rechtspraak/De_Juristenkrant/YAHOO%20Arrest%2030%20juni%202010.pdf?LangType=2067.

Articles

[1] Gutwirth, S., De Vries K. and Saelens, R., "Veiligheid legitimeert niet alle middelen", *Juristenkrant* 24 March 2010, 12.

[2] Van Linthout, P., "Yahoo is geen verstrekker van elektronische communicatiedienst", *Juristenkrant* 27 October 2010, 4-5.

[3] Order of Flemish Bar Councils, *Standpunt – Een kritische reflectie van de Europese databewaringsrichtlijn*, consulted via http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/20091026_Standpunt_Orde_van_Vlaamse_Balies.pdf, 2.