tion of personal data makes no sense; its aim was, rather, to point out that substantial questions remain unanswered over the basic conceptual features of the recent regulation and its European background.

Instead of discussing the real basics of the data protection regulations, their purpose and effects, we often tend to analyse only internal questions and problems. However, the concept is not so well-grounded in the legal system and in legal practice that we need to ask "Why should we not have this regulation." Instead, we should ask (analogically to Lessig's question about intellectual property rights): "Why should we have it?"

Personally, I think that there are, in fact, very solid grounds for argument in favour of the administrative protection of personal data. However, in order to reach the desired legitimacy at European and national level, the regulatory model needs to be confronted with these paradoxes and, consequently, reshaped. Otherwise, there is a danger of a conflict of validity[18] in which the law can never succeed.

Notes

* This article was created under the research project no. MSM0021622405.

1 As the core of the Radbruch's works was still not translated into English, we have to study his teachings from the secondary works – see for example Taekema, Sanne: The Concept of Ideals in Legal Theory, Kluwer Law International, The Hague, 2003. p. 69

2 Lessig, Lawrence: Free culture, Penguin Press, New York, 2004. p. 305

3 See for example Schwartz, Paul M.: Property, Privacy and Personal Data, In: Harvard Law Review, 2004. vol. 117(7), p. 2094

4 Brandeis, Louis D. – Warren, Samuel D.: The Right to Privacy, In: Harvard Law Review, 1890. Vol 4, p. 193

5 See for example Solove, Daniel J.: Conceptualizing Privacy, In: California Law Review, 2002. Vol 90, p. 1099

6 Ibid. p. 1109

7 Such an approach to the law was present in Europe namely at the end of the 19th and the beginning of the 20th century led by the German school of the so-called "Jurisprudence of Terms" (in German die Begriffsjurisprudenz).

8 While some of the national laws strictly define the personal data as only such that identify a living person, some of the laws including the harmonization directive do not solve the problem and leave the question open.

9 No further categories of personal data are used for example in the Cypriot Law "The Processing of Personal Data (Protection of Individuals) Law 138(I)2001.

10 As an example, we can use the Czech Act No. 101/2000 Sb., on "The Protection of Personal Data" and on "Amendments to Some Acts".

11 This example was taken from the Estonian Data Protection Act (RT I 2003, 26, 158).

12 This category is used by the Italian Personal Data Protection Code adopted by the Legislative Decree no. 196 of 30 June 2003.

13 Both defined in the Hungarian Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest.

14 The most important safe haven policy for EU companies was developed by the U.S. government on the grounds of the semi-private contractual basis – see the Safe Harbor page at the U.S. DoC Export Portal at http://www.export.gov/safeharbor/index.html [15.05.2007.]

15 The mere concept of principles of good governance was historically developed not legislatively, but by the courts arguing their interpretations of administrative laws making sense but being contrary to their black-letter wording. For a simple understanding of what the "reasonable application of the administrative law" means, we can unreservedly recommend the simple guide developed by the Australian government in an attempt to help developing countries – see Good Governance – Guiding Principles for Implementation, published by the Australian Government's Overseas Aid Programme, available on-line at http://www.ausaid.gov.au/publications/pdf/good_governance.pdf [15.08.2007.]

16 Very relevant formalist counterargument against, however wise and reasonable, interpretation contra legem is that, by allowing it, the state dissents from the rule of law in favour of the rule of men. Thus, there is a strong need for the respective 'men' to be equipped for the highest possible level of social and legal legitimacy. For the analysis of formalist arguments, see for example Posner, Richard Allen: Legal Formalism, Legal Realism and the Interpretation of Statutes and the Constitution, In: Case Western Law Review, 1986-1987. Vol. 37(2), p. 179

17 When the clerks are benevolent in such cases, it is in practice impossible to review or revise their interpretations – no one goes to the administrative court and asks for an additional obligation or punishment.

18 The conflict between legal (formal) validity and other types of validity was explained by Robert Alexy in Alexy, Robert: The Argument from Injustice – A Reply to Legal Positivism, Oxford University Press, New York, 2002. p. 83 Besides the conflict of legal and social or ethical validity, we also see now the emerging conflict between the legal and economic validity of laws which is dealt with by the popular stream in contemporary legal theory named "The Law and Economics".

Eleni Kosta – Jos Dumortier

Implementation Issues of the Data Retention Directive*

In March 2006 the European Union adopted a directive on the retention of traffic and location data which aimed to put an end to a vigorous debate on this issue among European Union institutions, industry players and privacy advocates. In this paper we shall offer a critical analysis of the detailed provisions of the directive in the light of the implementation procedures in the various Member States.

Eleni Kosta is a legal researcher at the Interdisciplinary Centre for Law & ICT (ICRI) of the K.U.Leuven, Belgium, and a doctoral candidate at the Faculty of Law of the same University, under the supervision of Prof. Jos Dumortier, on "Consent as a legitimate ground for data processing in electronic communications".
Jos Dumortier is Professor of Law at the K.U.Leuven, Belgium, and Director of the Interdisciplinary Centre for Law & ICT (ICRI). He is also a member of the Brussels Bar (time.lex)

1. Introduction

The retention of traffic and location data has been at the centre of discussion for several years within the European Union. Notwithstanding the existence of major differences in the approaches to the issue among the bodies of the European Union, privacy advocates and industry players [1], the European Union adopted in March 2006 a directive[1] to regulate it. However the debate regarding telecommunications data retention did not appear to stop. Ireland has challenged the directive before the European Court of Justice[2], arguing that the legal basis chosen for its adoption was not correct and that the relevant legal instrument should have been taken under the Third Pillar. The directive should be transposed into national law by the 15th of September 2007,

but it appears that the majority of e Member States will not complete the implementation procedures before this date.

2. The way to the directive

Although attempts to regulate the retention of traffic data for criminal investigation and prosecution purposes were introduced at least five years ago [2], the point of decision for the adoption of such a European legal instrument came with the terrorist attacks in Madrid. In fact, soon after the attacks took place, the Council in its declaration on combating terrorism of March 2004[3] considered the retention of communications traffic data by service providers as an adequate measure to combat terrorism and urged that proposals be made for establishing relevant rules, stressing that these proposals 'should be given priority with a view to adoption by June 2005'[4].

One month later, the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom prepared a proposal for the adoption by the Council of a 'Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism'[5]. This was the beginning of a very difficult period within the European Union. This was characterised by official but secret negotiations among the Council, the Commission and the European Parliament, as well as by serious opposition from civil liberties organisations[6] and industry actors, but it ended with the adoption of the recent Data Retention Directive.

The European Data Protection Supervisor (EDPS) issued an opinion on the Proposal for the Data Retention Directive[7] in which he stated that '[he] is as yet not convinced of the necessity of the retention of traffic and location data for law enforcement purposes, as established in the proposal'[8].

Moreover he gave his view that in order for the directive to be acceptable, the actual needs of law enforcement should be taken into consideration for the determination of the retention period or the data that are to be stored. Furthermore, he asked that the provisions of the directive respect the rights of the data subjects and general data protection principles.

However, the directive did not take into consideration all the recommendations and comments that were made by the EDPS. In fact, the aforementioned Opinion itself was not mentioned in the preamble to the Directive despite the fact that it was specified in the Opinion due to the mandatory character of Article 28 (2) of Regulation 2001/45/EC[9].

3. The Data Retention Directive

3.1. Retention of traffic and location data for law-enforcement purposes.

The scope of the Data Retention Directive is to ensure that traffic and location data, as well as data that are necessary to identify the subscriber or registered user, will be available for the purpose of 'investigation, detection and prosecution of serious crime, as defined by each Member State in its national law'. Contrary to the initial plans of the Council, the directive does not include the prevention of crimes within its scope of application.

3.2. How will Member States define 'serious crime'?

The directive does not include a definition of the term 'serious crime', a task which is left to the Member States to regulate in their national legislations. The Council urged Member States 'to have due regard to the crimes listed in article 2(2) of the Framework Decision on the European Arrest Warrant[10] and crime involving telecommunication'[11]. Nevertheless, due to the fact that each Member State is to define serious crime individually, deviations in the scope of application of the directive are to be expected. The demands already expressed in Germany illustrate how the definition of 'serious crime' can be stretched and provide a powerful argument to the effect that Member States should be very careful when they transpose the directive into their national legislation.

The Director of the German Chapter of the International Federation of Phonogram and Videogram Producers (IFPI) called for the rapid implementation of the Data Retention Directive so that data records could be made available for civil law disclosures and file-sharers could be traced. This demand produced a reaction from Hannes Federrath, Professor of Information Security Management at the University of Regensburg, who reminded the representatives of rights-holders that "what [they] are demanding here goes beyond what prosecutors of consumers of child pornography get". [12]

3.3. Who has an obligation to retain data?

The directive aims at the harmonisation of the obligations of providers of publicly available communications services or public communication networks. The terms 'electronic communications network'[13] and 'electronic communications service'[14] are defined in article 2 (a) and (c) of the Framework Directive[15] respectively. The wording of the definitions can lead to a very broad interpretation of the term and so to a very broad group of providers who qualify as 'providers of public communications networks'. In any case, the directive missed the opportunity to define the term 'providers of publicly available communications services or public communication networks' in detail and avoid differing interpretations among Member States. The Article 29 Working Party has also identified the need for clarification of these two terms, stating explicitly that "both definitions 'electronic communications services and 'to provide an electronic communications network' are still not very clear and that both terms should be explained in more detail in order to allow for a clear and unambiguous interpretation by data controllers and users alike"[16]

According to recent data retention legislation in France, the data retention obligations apply to Internet cafés, hotels, restaurants, and, generally, to any person or organisation providing Internet access, free or for a fee, as a main or side activity[17]. In Italy internet cafés are already obliged to ask for an identification document from any of their customers and, further, to log the owner's name and the type of the identification document[18]. The German draft is currently considering anonymisation services as providers who will have to retain data, so making them, in practice, superfluous.

Recital 13 of the Data Retention Directive states that "data should be retained in such a way as to avoid their being retained more than once". However, this is not obvious in practice, especially with regard to internet services. In order to use a service on the internet, users make use of services provided by several different providers at the same time, and they may use different access providers to access the same service. In such a context it becomes rather cumbersome to define who shall be the provider to retain which data. This issue seems to have been in time identified by some Member States, such as Sweden, that are preparing legislation that takes account of the layered structure of services on the internet and will most likely make detailed provisions regulating which providers will have to retain which types of data.

3.4. What data are to be retained?

The Data Retention Directive calls for the retention of traffic and location data as well as any related data necessary to identify the user or the subscriber, whilst no content data shall be retained. The directive asks also for

the retention of data relating to unsuccessful call attempts (Art. 3(2) DRD), although the Article 29 Working Party had expressed an opinion to the contrary[19]. However, neither data relating to unconnected calls (Art. 3(2) DRD) nor data relating to web browsing [3] are to be retained.
The above-mentioned data are retained when they are generated or processed and stored (for telephone data) or logged (for internet data) by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communication services concerned (Art. 3(2) DRD). Although the defenders of the directive claim that the providers will not need to retain more data than those already generated or processed in the process of supplying their communications services (Art 3 (1) DRD), it can also be argued that, when providers offer flat-rate charging systems, they would not need to retain data at all, as the latter would not be needed for billing purposes.

3.4.1. Types of data to be retained
The Data Retention Directive, however, does not ask for the retention of any traffic data generated or processed by the provider, but includes a detailed list with the categories of data to be retained in Art. 5. The main categories of these data include:
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 or what purports to be their equipment;
f) Data necessary to identify the location of mobile equipment.
Although article 5 contains a very detailed list of the data that are to be retained by the providers, this solution is criticised as being very rigid to adjust to new technologies. In the Proposal of the Directive[20], it was provided that only general categories of data would be included in the text of the directive, whilst a detailed list would be attached as an Annex. For the revision of the Annex, a Comitology procedure[21] was envisaged (Art. 6 Proposal DRD). This approach seems to be being followed by the Netherlands, who will not include a detailed list of the data to be retained in the body of the relevant law, but will incorporate them in an Annex which can be modified by an administrative decree by following a simpler procedure.

3.5. Retention period

3.5.1. 'Normal' retention period: 6 to 24 months
One of the main goals of the directive was to harmonise retention periods, which differ significantly among those Member States which already have data retention legislation. In Italy, for example, telephone traffic data is to be retained by the provider for twenty-four months for the detection and suppression of criminal offences. This may be extended to forty-eight months, exclusively with a view to detecting and suppressing organised crime, Cybercrime and crimes committed within an organisational (mafia) structure or for services delivered by a citizen to a hostile state[22]. Irish legislation allowed the Garda Commissioner (Ireland's National Police Commissioner) to request service providers to retain data for a period of 3 years for specific purposes and disclose them when asked[23]. Poland has even called for a new law to introduce mandatory telephony data retention for 15 years, following a complaint from local investigators that they are unable to prosecute corruption effectively without telephone billing data from the last 4 years.[24]
The directive tries to put an end to these wide variations and provides for the data to be retained for periods of not less than 6 months and for a maximum of two years from the day of the communication (Art. 6 DRD). This choice can be seen as in the middle of the suggested retention periods included in the Draft Framework Decision of April 2004 and the Commission Proposal for a Data Retention Directive.
Art. 15 (3) of the directive allows Member States to postpone the application of the directive 'to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail' until 36 months following the date of adoption of the directive. 16 member-states have taken advantage of this derogation and have declared their decision to postpone the retention of such data, together with Romania and Bulgaria who joined the EU after the adoption of the directive.[25] These Member States used various forms of wording in their declarations: some are to postpone retention for 36 months following the adoption of the directive, others for 18 months from the incorporation of the directive into their national legislation (which, very probably, will not coincide with the 36 month-period) and others have included no specific period of time in their declarations.
The first EU Member-State to implement the directive is Slovenia, which has opted for a retention period of not less than 24 months. However, most countries (e.g., Denmark and the UK) seem to have chosen a retention period of 12 months. The Dutch draft for the implementation of the Data Retention Directive asked for data retention for 18 months, but this choice was criticised by the Dutch Data Protection Authority, which claimed that the proposed period had not been demonstrated satisfactorily[26]. Germany has opted for the minimum retention period of six months.

3.5.2. Extension beyond the maximum period of 24 months: when and for how long?
The Data Retention Directive allows Member States to extend the maximum retention period, when facing particular circumstances (Art. 12 DRD). As soon as they take such a measure, they are to notify the European Commission and inform other Member States of the measures taken, indicating the grounds for introducing them. Within six months the Commission shall approve or reject the imposed national measures.
Article 12 (3) further describes the impact which these measures may have in the retention of data at European level. Following the approval of the abovementioned national measures which derogate from the provisions of the Data Retention Directive, the Commission may examine possible amendments to the directive itself. This provision is to be used "exceptionally and prudently", since it can be used as a 'Trojan horse' for future radical adaptations to the Data Retention Directive [3].

3.6. Who can have access to the retained data

The retained data shall be provided only to the competent national authorities in specific cases and in accordance with national law, according to Art. 4 DRD. Working Party 29, in order to avoid confusion regarding which authorities fall under the term 'competent national authorities', proposed the creation of a list of designated law enforcement services which should be made public.[27]
In France the relevant legislation allows only judicial authorities, together with police forces, to access the retained data.[28] However in the UK the situation is not so clear. The Regulation of the Investigatory Powers Act 2000 (RIPA) provides that 'relevant public authorities' can access the retained communications data. The Regulation of Investigatory Powers (Communications Data) Order 2003 allowed a large number of official bodies to have access to retained data [4].
Access to retained data is an attraction pole not only for national public authorities, but also for countries outside the European Union who will attempt to access these data. During the EU-US Informal High Level Meeting on

Freedom, Security and Justice which took place in Vienna the USA expressed interest in obtaining access to the data to be retained according to the Data Retention Directive[29].

3.7. Impact on the industry

The retention of data as described in the Data Retention Directive imposes severe obligations on providers. The providers must, inter alia, comply with four fundamental obligations laid out in Article 7 DRD. They must ensure that the retained data are of the same quality and subject to the same security and protection as those data on the network. Furthermore, the data shall be subject to appropriate technical and organisational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure. Appropriate measures shall also be taken in order to ensure that they can be accessed by specially authorised personnel only. Finally, all other data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

This last obligation could be further interpreted as the beginning of the Odyssey of the providers regarding the deletion of data. Although such an obligation already existed in data protection legislation, the industry players were not very vigilant in deleting data, especially given the tolerance shown by the Supervisory Authorities. The Data Retention Directive, however, obliges the providers to delete the data following the end of the retention period. This could be translated in simple language as an obligation for the providers to erase (or make anonymous) the data that are needed for billing purposes after the end of the period specified in national legislation. However, if some of these data fall under Article 5 of the Data Retention Directive, the provider is to retain them and delete them finally following the end of the retention period.

As early as August 2005, the German Industry issued a paper with 'Demands for a Debate on Europe-wide Compulsory Data Retention'[30], asking for the full reimbursement to industry of the costs of any data retention - to cover both investment costs as well as operating costs[31]. The solution given by the directive totally fails to fulfil this request in that the directive does not provide for the reimbursement of any additional costs incurred by the industry in order to comply with data retention legislation.

However, the European Commission has expressed the opinion that 'reimbursement by Member States of demonstrated additional costs incurred by undertakings for the sole purpose of complying with requirements imposed by national measures implementing this directive for the purposes as set out in the directive may be necessary'[32]. A similar provision was included in Art. 10 of the Commission's proposal for the Data Retention Directive, but was deleted from the final text. Although such reimbursement could, therefore, be granted as legitimate state aid, and so fully comply with Articles 87 et seq. of the EC Treaty, the Member States are not obliged by the Data Retention Directive to reimburse these costs.

In addition to the additional operating costs which European providers suffer, users might also become more sceptical of using the offered services. For example, a privacy-sensitive user would prefer to use a provider established outside the EU as opposed to a European one, as the former will not retain so much of his data [5].

A further point of criticism of the directive is the fact that it does not take into consideration the particularities of the internet. The typical internet-user leaves a 'trail', creating traffic data which can reveal much more information about his habits and interests than data on a person who was contacted by telephone.[33] Moreover, the volume of Internet data created is extremely large and providers will need adequate systems with enough storage capacity in order to store and organise the data to be retained[34].

4. Conclusion

Even though it takes great care and effort to build a house of cards, it may collapse or tumble down at any moment. Concerns for the directive in question are similar.. Its final adoption might, after all, not be the final step in establishing a common data retention regime among EU Member States: national courts may 'challenge' the directive, a scenario which seems very realistic in the case of Germany under the influence of the jurisprudence of its Constitutional Court.

Ireland has already challenged the directive before the European Court of Justice, arguing that the retention of traffic and location data should have been regulated via a Council decision under the Third Pillar. This argumentation seems to have strengthened recently after the PNR Judgement of the European Court of Justice[35] which gave a new interpretation of the use of personal data for law enforcement purposes. Pursuant to the reasoning of the Judgement, data processing necessary for safeguarding public security and for law enforcement purposes falls within the exceptions listed in Article 3(2) Data Retention Directive[36], and so the European Community is not competent to regulate such issues under the First Pillar. This Judgement may have an impact on the Data Retention Directive, should the Court be required to pronounce on the legal basis of the directive.[37]

Notes

* This paper is a substantially revised and updated version of the paper given at the FITCE 2006 Congress.

1 Directive 2006/24/EC of the European Parliament and of the Council 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, Official Journal L105, 15 March 2006, p. 54

2 European Court of Justice, C-301/06: Ireland v Council and Parliament, O.J.E.U. C 237/5, 30 September 2006

3 http://register.consilium.eu.int/pdf/en/04/st07/st07906.en04.pdf

4 Ibid.

5 http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf

6 Inter alia http://www.dataretentionisnosolution.com/, http://www.edri.org/issues/privacy/dataretention

7 Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005) 438 final), OJ C 298, 29 November 2005, p. 1

8 Ibid

9 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal L 008 , 12 January 2001 P. 0001 – 0022

10 Council Framework Decision on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) (13 June 2002)

11 Council of the European Union, Statements, Council doc. 5777/06 ADD 1 (February 10, 2006) available at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf

12 http://www.heise.de/english/newsticker/news/71866

13 Electronic communications service is defined as: '[…]a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'.

14 'Electronic communications network' means '[…] transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed' .

15 Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108, 24 April 2002, pp. 33-50

16 Article 29 Working Party, Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, 26 September 2006, p. 3, available at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf.

17 Law 2006-64 of 23.01.2006 on the fight against terrorism, including provisions regarding security and border controls [Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrőles frontaliers], available at http://foruminternet.org/documents/lois/lire.phtml?id=998

18 http://www.edri.org/edrigram/number3.16/Italy

19 Article 29 Working Party, Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 21 October 2005, p. 9, available at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf.

20 Proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, 21 September 2005, available at http://www.europa.eu.int/information_society/policy/ecomm/doc/info_centre/communic_reports/data_retention/retention_proposal_en_com_2005_0438.pdf.

21 A Committee composed of representatives of Member States and chaired by the representative of the Commission would assist the Commission in the revision of the Annex on a regular basis.

22 Art 132 Italian personal data protection code [Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali], available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1105372

23 Section 63 of the Irish Criminal Justice (Terrorist Offences) Act 2005, available at http://oireachtas.ie/documents/bills28/acts/2005/a0205.pdf

24 http://www.edri.org/edrigram/number3.24/Poland.

25 The declarations of the 16 countries can be found at the end of the Directive.

26 Opinion of the Dutch Data Protection Authority [College bescherming persoongegevens (CBP)], Legislative proposal (Bill) for the implementation of the European Directive on Data Retention, Pertaining to the tender letter of 22 January 2007, 24 January 2007, p. 2

27 Article 29 Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council 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, 25 March 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf.

28 French decree no. 2006-358 regarding the retention of electronic communications data [Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques], available at http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSD0630025D

29 http://www.statewatch.org/news/2006/apr/eu-us-jha-7618-06.pdf

30 http://www.bitkom.org/files/documents/Stellungnahme_BDI_BITKOM_VATM_Vorratsdatenspeicherung_DE_05_08_05.pdf

31 See also the case in France where the French Association of Internet Access and Service Providers (AFA) announced that it would challenge the decree no. 2006-358 regarding the retention of electronic communications data before the 'Conseil d'Etat' http://www.afa-france.com/p_20060328.html

32 Council of the European Union, Statements, Council doc. 5777/06 ADD 1 (10 February 2006) available at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf

33 Commission Staff Working Document 'Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC EXTENDED IMPACT ASSESSMENT', 21 September 2005, available at http://www.statewatch.org/news/2005/oct/com-dataret-reg-ass-05.pdf, pp. 13-14

34 A Dutch Internet Service Provider, xs4all, counted that its traffic between 5 September 2005 and 14 June 2006 is 150.677.000.000.000 data packets, which are approx. 131.996.000 CD's. You can find the counter at http://www.xs4all.nl/bewaarplicht/

35 Judgement of the Court of Justice in Joint Cases C-317/04 and C-318/04

36 Directive 1995/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 0031 – 0050 (23 November 1995).

37 Other references:
[1] Walker, Clive – Akdeniz, Yaman: Anti-Terrorism Laws and Data Retention: War is over? In: Northern Ireland Legal Querterly, 2003/2, pp. 159-182
[2] Munir, Abu Bakar: Retention of communications data: Security vs Privacy. Paper presented at Oxford Internet Institute Conference: Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities, 8 September 2005, http://www.oii.ox.ac.uk/research/cybersafetyextensions/pdfs/papers/abubakar_munir.pdf [17.11.2005.]
[3] Kosta, Eleni – Valcke, Peggy: Retaining the Data Retention Directive. In: Computer Law & Security Report, 2006/5, pp. 370-380
[4] Munir, Abu Bakar – Yasin, Siti Hajar Mohd: Access to Communications data by public authorities. In: Computer Law and Security Report, 2004/3, pp. 194-199
[5] Memorandum of laws concerning he legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, October 2003. Prepared by Covington & Burling LLP, http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf. [12.12.2006.]

NATALIE FERCHER

National Implementation of the Data Retention Directive in Austria

1. Introduction

The Data Retention Directive[1] imposes obligations on providers to retain traffic and location data. The data in question relate to the use of mobile and fixed telephony as well as to the Internet communication of all users. The main aim is to ensure that data are available for the purposes of investigating, detecting and prosecuting serious crimes, as defined by national law.

This is obviously a paradigm shift. In 2002 there came into force the Directive on Privacy and Electronic Communication[2], whose aim was to ensure user privacy regarding specific risks arising from new technologies. As a general principle, the quantity of personal data necessary should be limited to a strict minimum, and so the existing legal framework explicitly protects citizens' privacy and personal data and provides for the deletion of traffic data once no longer needed for the purposes of conveying communication or billing.

The author works as research assistant at the Department of Information Technology Law and Intellectual Property Law, Vienna University of Economics and Business Administration